COMMERCIAL BANKING

CARDNET

Card payments made easy for you and your customers

LLOYDS BANK

Contents

Welcome	1
1. Key points	3
2. Acceptable cards	5
Visa	7
Visa Credit	9
Visa Debit	9
V PAY	11
Visa Electron	13
Visa Prepay	15
Visa and Visa Electron mini cards	15
Visa SimplyOne card	15
MasterCard®	17
Debit MasterCard	18
Maestro®	19
Discover®	21
Diners Club International®	23
BC Global Card	25
DinaCard	26
Contactless	30

Contents

Commercial cards	31
3. Checking the card	33
Security features	34
Additional checks	38
4. Accepting transactions	39
Over the counter transactions	40
Card Not Present (CNP) transactions	43
Address Verification Service	46
E-commerce	50
Card schemes	53
5. Authorisation and referrals	55
When to obtain authorisation	56
Manual authorisation	56
Authorisation adjustments/reversals	56
Referrals	57
Split sales with cash, cheque or second credit card	57
Cancelling a transaction	58
Refunds	58

Contents

6. Banking and reconciliation 59
Electronic data 60
Paper vouchers 60
Record keeping 62
Your Cardnet statement 63
Online reporting tool 63
7. Security 65
Data security 66
Payment Card Industry – Data Security Standards (PCI DSS) 67
Protecting your point of sale and card processing equipment 70
Suspicious transactions 73
How to guard against fraud 75
Chargebacks 81
8. Additional facilities for you and your customers 87
Purchase with Cashback 88
Mobile phone top-up 88
Recurring transactions 89
Polling 91
Gratuities 91
Dynamic Currency Conversion (DCC) 92

Contents

Accepting currency transactions	**92**
Cash Advance	**92**
Additional cards	**92**
9. Exceptions	**93**
Failed chip card read	**95**
Failed magnetic strip transactions	**95**
Using the paper fallback system	**97**
10. Additional information	**103**
Notifying us of changes to your business	**104**
How to complain	**105**
What to do if you experience financial difficulties	**107**
Agencies offering financial assistance	**109**
Authorisation telephone numbers	**110**
Merchant services	**110**
Cardnet stationery	**110**
Point of sale and display material	**110**
Recommended tally roll supplier	**111**
Cards left on your premises	**111**
Emergencies and disruptions	**112**

Taking card payments should be simple and convenient for my business and customers

Security, flexibility and convenience – welcome to Cardnet®

Thank you for choosing Cardnet®. At Lloyds Bank Commercial Banking, we serve around 1 million UK businesses and understand what you need from your card processing system. Cardnet is one of the UK's largest payment processors and offers you rapid transaction handling and payment reconciliation. You'll be able to accept payments from one of the widest ranges of card schemes available.

This manual will help your business make the best use of Cardnet features and services. In it you will find all the information and procedures needed to be sure of using Cardnet easily and securely, and conducting your banking as efficiently as possible.

The manual forms part of your agreement with Cardnet, so please read it and make sure it is retained in a safe place and available for all relevant staff to refer to.

Please contact us if you'd like this information in an alternative format such as Braille, large print or audio.

CARDNET HELPLINE

Call 01268 567 100
8am to 9pm Monday to Saturday
Call our knowledgeable UK-based team with any questions about your Cardnet service or this manual.

85,000

Cardnet terminals in operation

1.3 million

transactions processed by Cardnet every day

1 : Key points

To get the most out of the Cardnet service, it is important to follow some basic procedures that are strictly enforced by Visa, MasterCard, Maestro and Discover Financial Services.

You must

- Display Visa, V PAY, MasterCard®, Maestro® and, where applicable, other scheme logos (for example Diners Club International®) on promotional materials.
- Prominently display any surcharge you impose at point of sale (POS). Any surcharge must be included in the transaction amount and not processed separately.
- Include any taxes in the amount charged on card transactions. They may not be collected by you in cash.
- Provide the cardholder with the option of receiving confirmation of the transaction for their records. This need not be a separate receipt. The card payment data can be included at the bottom of your POS itemised receipt. With chip and PIN-capable POS, the information displayed should include an indication that it is PIN verified. Only the last four digits of the card number are to be shown on the cardholder's copy.
- Only make cash disbursements to a cardholder as part of a card transaction up to the limit authorised in your agreement with us.
- Have prior written agreement from Cardnet before accepting mail/telephone order or E-commerce card transactions.

You must not

- Indicate that Cardnet, Visa, MasterCard, Discover Financial Services, its partner cards or any other association endorses your goods and services.
- Establish minimum or maximum amounts as a condition for accepting a card.
- Impose a surcharge on Visa debit cards (this is a Visa scheme requirement).
- Submit a transaction or sale that has previously been charged back. See Section 7, 'Security, Chargebacks'.
- Accept any direct payments from cardholders, for example, cash/cheques for the credit of the card account (only the card-issuing bank is authorised to receive such payments).
- Process paper transactions except in the case of fallback. See Section 9, 'Exceptions', page p93.
- Accept transactions on behalf of third parties.
- Discourage, favour or discriminate against the use of any particular card which is part of a Card Scheme you have agreed to accept.
- Store magnetic stripe data that facilitates card processing or Card Security Code (CSC) details. Special Card Scheme regulations apply if you (or your agent) store this data electronically and failure to comply with these requirements may result in a fine.

2 : Acceptable cards

This section details the features to look for when accepting cards.

You will have agreed separately with us the card types you are able to accept

It is important to check the cards thoroughly to help prevent card fraud. The following descriptions will help you and your staff to check a card's validity and to follow the correct card acceptance procedures.

If a card does not fit these descriptions, it must not be accepted. If you have any doubts or if you are suspicious, contact the Authorisation Centre on **01268 822 822** and ask for a Code 10 authorisation. See Section 7, 'Security, Suspicious transactions' (p73).

AUTHORISATION CENTRE

Call 01268 822 822
State "This is a Code 10 call" and follow the operator's instructions.

VISA

These card images are for visual purposes only.

Visa cards are produced in many different designs and each card identifies the issuer. All Visa cards have the Visa logo on the front of the card. The position of the logo depends on the card type.

The card has the following features:

1 Visa logo – The blue and gold logo on a white background will be displayed on the front of all Visa cards.

2 Chip – Most cards carry an embedded chip which works together with the cardholder's PIN or signature.

3 Visa 3D dove hologram – A dove in flight which moves and changes colour when tilted. This can be located on the front or on the reverse of the card.

4 Embossed or printed account number – The embossed or printed account number, which can be up to 19 digits.

Some unembossed Visa cards may only be printed with a partial account number.

All or part of the account number must match the printed account number on the sales receipt.

5 Cardholder name – Most Visa cards will carry an embossed or printed cardholder name, which may also include their title.

6 Printed BIN (Bank Identification Number) – The four-digit printed BIN number must appear below the account number and must match the first four digits of the embossed or printed account number.

7 Expiry date – Every Visa card must have an expiry date. Some may also include an optional 'Valid From' date.

8 Ultraviolet mark – When placed under an ultraviolet light newer Visa cards will have a 'V' visible over the Visa logo. On older cards a dove will appear in the centre of the card.

9 Magnetic stripe – The magnetic stripe holds information about the card and appears on the back of all cards.

10 Card Security Code (CSC) – The three-digit security code may appear:
   - On the signature strip next to the full card number or card number showing only the last four digits.
   - Alternatively it may appear in a white box beside the signature strip.

11 Signature strip – The signature strip may be customised and may vary in length from card to card. On some older cards it may still extend the entire width of the card. The last four digits of the card number, together with a three-digit Card Security Code, will appear on the right-hand side. Some older cards in circulation may show the whole account number followed by the three-digit Card Security Code.

It is now optional on current Visa cards for the 'flying V' (the letter V tilted to the right) to appear next to the expiry date on the front of the card.

Visa Credit

Visa Debit

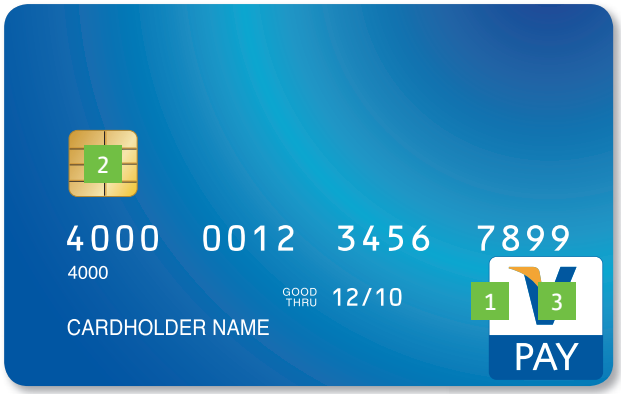
AUTHORISED SIGNATURE – NOT VALID UNLESS SIGNED BELOW
1234 123
0845 3 000 000
Any problems using your card abroad call
+44 1733 347 007
You can use your debit card:
• Abroad on your holiday
• Online for goods and services
• Shopping on the high street
lloydsbank.com

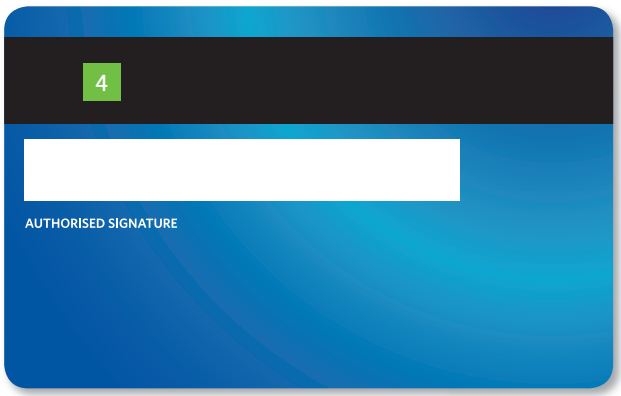
These card images are for visual purposes only.

Speed and convenience

Cardnet makes payment faster and easier for you and your customers.

V PAY





These card images are for visual purposes only.

V PAY is a Visa debit card issued by banks from around Europe to their customers. The big difference with V PAY is that it is a chip and PIN only card, so it is very easy to accept and the risks of fraud and associated disputes are greatly reduced.

V PAY cards mandatory features:

1 V PAY logo – The V PAY logo is the blue and gold Visa logo on a white background and can be displayed in three locations on the front of the card (upper left, upper right or lower right).

2 Chip – is located on the front of the card. Cardholders are required to enter a PIN to make a purchase.

3 Ultraviolet mark – when placed under an ultraviolet light, a 'V' printed in ultraviolet ink is visible over the V PAY logo.

4 Magnetic stripe – holds information about the card and appears on the back of all cards.

Optional features:

Features that can appear on the front or back of the card:

- The cardholder's name.
- The expiry date.
- Cardholder number – the unembossed number can be between 16 and 19 digits.
- Issuer identification (bank name) – may appear on the front or the back of the card.
- Contactless indicator – can be displayed in Visa blue, black or white.
- Cardholder photograph.
- Domestic Debit Scheme mark.

Features that only appear on the front of the card:

- Printed BIN (Bank Identification Number) – The four-digit printed BIN number must appear below the account number and must match the first four digits of the printed account number.

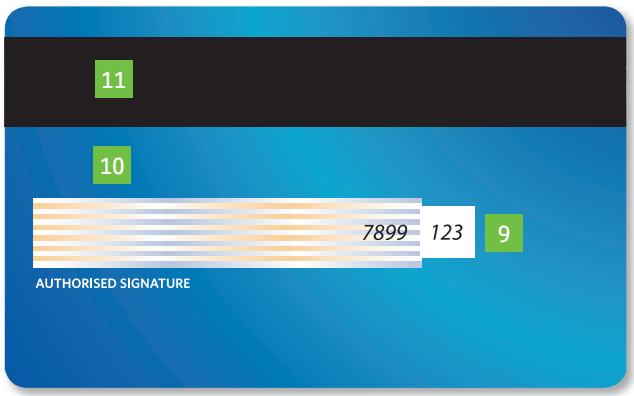
Features that only appear on the back of the card:

- Signature strip – can be customised and can vary in length from card to card.
- Plus symbol – allows ATM services.
- Card Security Code (CSC) – three-digit security number.

Important

- Authorisation – All V PAY transactions must be authorised – either online or offline – at the time of the transaction.
- Internet (E-commerce) V PAY cards can be used to make purchases over the Internet if permitted by the issuer. However, you must be registered for Verified by Visa to be allowed to display the V PAY logo on your website.
- Mail order/telephone order and recurring transactions – V PAY cannot be accepted for mail order/telephone order or recurring transactions.

Visa Electron



These card images are for visual purposes only.

1 Visa Electron logo – Always appears on the front of the card, usually on the right-hand side.

2 'Electronic Use Only' legend – Visa Electron cards are printed with the wording 'Electronic Use Only' and this may appear on either the front or the back of the card.

3 Chip – Most cards carry an embedded chip which works together with the cardholder's PIN or signature.

4 Account number – 16-digit account number with first four digits printed below. Not all cards show the full account number, however, in the UK the full account number is required.

5 Cardholder name – This is always unembossed and appears on the front of the card. The cardholder's title may also be present.

6 Hologram – The hologram is optional for Visa Electron cards and features a dove in flight which moves and changes colour when tilted. This may be located on the front or on the reverse of the card.

7 Expiry date – Every Visa card must have an expiry date. Some may also include an optional 'Valid From' date.

8 Ultraviolet mark – When placed under an ultraviolet light newer Visa Electron cards will have a 'V' visible over the Visa logo. On older cards a dove will appear in the centre of the card.

9 Card Security Code (CSC) – The Card Security Code will only be present if the full account number appears on the front of the card. If present, the Card Security Code may appear on or to the side of the signature strip.

10 Signature strip – This may appear in the traditional position or lower and may vary in length. Visa Electron is a globally accepted payment card and all transactions must be authorised regardless of the amount. In the UK, the Visa Electron will be primarily issued as a debit card and will have the full account number printed on the front.

11 Magnetic stripe – The magnetic stripe holds information about the card and appears on the back of all cards.

Important

- Over the counter transactions – As the Visa Electron card can only be accepted electronically, it must be inserted into the chip reader or swiped through the terminal in a card present environment. It cannot be key entered or accepted on paper vouchers even for fallback if your terminal is not working.
- Card Not Present transactions – In a Card Not Present environment, key entry is permitted.
- E-commerce transactions – Visa Electron can be accepted over the Internet.

The above procedures must be adopted for all Visa Electron payments. If these procedures are not followed we reserve the right to chargeback any transaction.

Visa Prepay

Visa issues prepay cards where funds have been preloaded onto the card. These cards carry the Visa logo and should be treated the same as a Visa debit card.

Visa and Visa Electron mini cards

Visa has produced miniaturised Visa and Visa Electron cards. These cards carry the Visa and Visa Electron logos in reduced sizes positioned in either the bottom or top right of the card.

The Visa mini dove hologram will always appear on the Visa card but is optional on the Visa Electron mini card.

The mini dove hologram can appear on either the front or the back of the card.

Other features include:

Signature strip

A signature strip can be found on the back of the card.

Magnetic stripe

The magnetic stripe can be found on the back of the card.

Card Security Code

The three-digit security code may appear on the signature strip next to the full card number (or alternatively the last four digits from the card number) or it may appear in a white box beside the signature strip.

Cardholder photograph and signature

A photograph of the cardholder may appear on either the front or back of the card.

Visa SimplyOne card

The Visa SimplyOne card is a multiple payment chip card that will provide cardholders with two (or more) payment applications (for example, debit and credit) on a single chip card.

The card design has two card numbers and two Card Security Codes. The card number for the main functionality is embossed on the front of the card with a corresponding Card Security Code positioned beside the signature strip on the reverse of the card. The secondary card number and Card Security Code are printed on the reverse of the card.

Both card functions share the same validity dates.

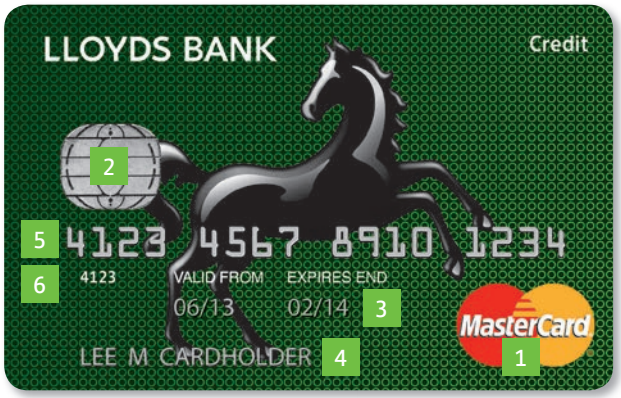
A card that is both a debit and a credit card will have 'Debit/Credit' printed below the Visa logo on the front of the card. This card will allow the cardholder to choose at the point of sale whether to use the card as a debit or a credit card.

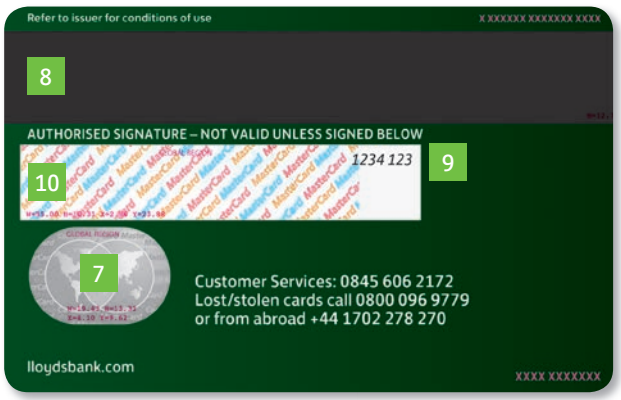
For further information about Visa and its interchange rates **visit www.visaeurope.com**

The efficient way to trade

Rapid, secure transactions and easier payment reconciliation.

MasterCard®





These card images are for visual purposes only.

MasterCard® cards are produced in many different designs and each card identifies the issuer. All MasterCard cards have the MasterCard logo on the front of the card.

All MasterCard cards carry the following features:

1 MasterCard logo – The MasterCard symbol of two interlocking globes and the MasterCard hologram will appear together surrounded by a retaining line on the front of the card. Alternatively the two interlocking globes will appear on the front of the card and the hologram will appear on the back.

2 Chip – Most cards carry an embedded chip which works together with the cardholder's PIN or signature.

3 Expiry date – Every MasterCard card must have an expiry date. Some may also include an optional 'Valid From' date.

4 Cardholder name – Most cards carry an embossed or printed cardholder name and may also include their title.

5 Embossed or printed account number – The embossed or printed account number, which can be up to 19 digits.

All or part of the account number must match the printed account number on the sales receipt.

6 Printed Bank Identification Number (BIN) – The four-digit printed BIN number must appear below the account number and must match the first four digits of the embossed or printed account number.

7 MasterCard 3D interlocking globe hologram – The hologram can appear on the front or the back of the card and shows two interlocking globes which move and change colour when tilted.

8 Magnetic stripe – The magnetic stripe holds information about the card and appears on the back of all cards.

9 Card Security Code (CSC) – The three-digit security code may appear on the signature strip next to the full card number (or alternatively the last four digits from the card) or it may appear in a white box beside the signature strip.

10 Signature strip – Many cards will carry a shortened signature strip; however, on some older cards it may still extend the entire width of the card. The signature strip is tamper-evident and will always be printed with a MasterCard repeat pattern.

It is now optional on current MasterCard cards for the letters 'MC' tilted to the right to appear next to the expiry date on the front of the card.

Debit MasterCard

Maestro®

These card images are for visual purposes only.

Maestro® is the debit card brand owned by MasterCard and is issued by many different banks, both in the UK and overseas.

All Maestro cards identify the issuer and feature the standard blue and red Maestro logo on the front of the card.

Usually cards will carry the following details:

1 Maestro logo – the blue and red interlocking circles with the word 'Maestro' printed across the centre in white.

2 Cardholder number – this can be between 12 and 19 digits.

3 The cardholder's name.

4 The expiry date.

5 The magnetic stripe.

6 Signature strip – this may be printed with the word 'Maestro' in repeat pattern and may also contain the last four digits of the cardholder number followed by the three digit Card Security Code.

7 Card Security Code (CSC) – The three-digit security code may appear on the signature strip next to the full card number (or alternatively the last four digits from the card) or it may appear in a white box beside the signature strip.

Please note, there are some fundamental differences in the appearance of UK Maestro cards and internationally issued Maestro cards.

Some may also contain the following:

- The chip.
- The hologram.
- The cardholder's title (for example, Mr, Mrs, Miss).
- The start date.
- The card issue number – this is the sequential number used to identify cards issued on the same account. It will be one or two digits only.
- Cheque guarantee and ATM functionality.

There are also some differences in the way UK Maestro and internationally issued Maestro cards operate and it is very important that you follow this manual for all Maestro cards you accept.

Please ensure that your staff are trained to accept Maestro cards, and are familiar with these procedures.

Maestro

Maestro transactions must always be processed through your terminal. Some Maestro cards have additional functionalities such as cheque guarantee and ATM.

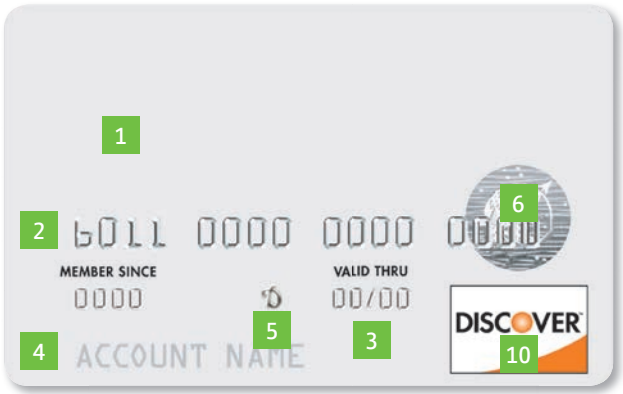
International Maestro

All internationally issued Maestro transactions must be authorised and your terminal will recognise this. (In the event of failed card read or swipe, please refer to the terminal fallback procedures set out in Section 9, 'Exceptions'.)

If you accept E-commerce transactions you must be registered for MasterCard SecureCode before you can accept any Maestro or International Maestro cards.

For further information about MasterCard and its Interchange rates visit **www.mastercard.us/merchants/support**

Discover®



These card images are for visual purposes only.

Discover® is a product of Discover Financial Services and is one of the largest issuers of cards in the US. Since its inception in 1986, Discover has been recognised as America's pioneer in cash rewards.

1 Ultraviolet mark – 'DISCOVER' or 'DISCOVER NETWORK' will appear under an ultraviolet light.

2 Embossed or printed account number – All Discover account numbers start with 6. Embossed card numbers should be uniform in size and spacing, and extend into the hologram. Unembossed cards may display account number and expiration date printed flat on the front.

3 Expiry date – 'Valid Thru' indicates the last month in which the card is valid.

4 Cardholder name – Normally the name of the cardholder will be embossed on the card. In some cases a business name may also be embossed below the account name.

5 Security character – Embossed security character appears as a stylised 'D'. The stylised 'D' does not appear on unembossed cards.

6 Hologram – All cards display a hologram on the card front with a globe pierced by an arrow, unless the card back displays a holographic magnetic stripe.

7 Magnetic stripe – Newer cards display a three-dimensional holographic magnetic stripe which (when tilted) shifts colour and appears to move.

8 Signature strip – 'DISCOVER' or 'DISCOVER NETWORK' appears on a tamper-evident signature panel. The last four digits of the card number are displayed on the signature panel in reverse indent printing.

9 Card Security Code – The three-digit CSC is printed in a separate box to the right of the signature panel on the card back.

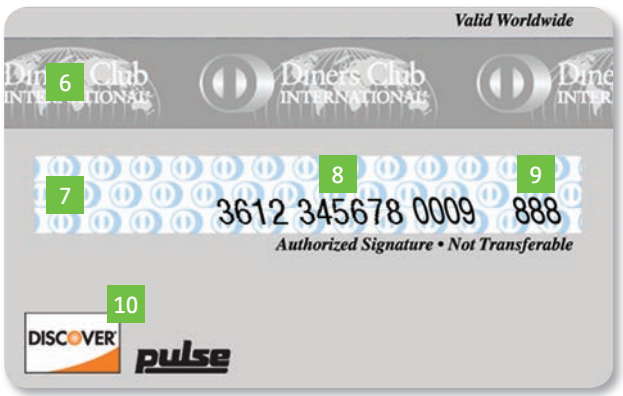
10 Discover acceptance mark – The Discover or Discover Network acceptance mark will appear on the front AND/OR back of the card.

CARDNET HELPLINE

Call 01268 567 100

8am to 9pm Monday to Saturday
Call our knowledgeable UK-based team with any questions about your Cardnet service or this manual.

Diners Club International®



These card images are for visual purposes only.

Diners Club International® is a product of Discover Financial Services and is a globally recognised brand serving the needs of consumers, corporations and small business owners worldwide. The cards come in many different designs (including some with the cardholder's photo on the front or back of the card), all have the Diners Club International logo on the front of the card and co-branded cards may also display the co-branded logo in the upper right-hand corner.

Some corporate cards may also have the words 'Corporate Card' or 'Business Card' and the company or corporate name displayed on the front of the card.

1 Ultraviolet mark – The Diners Club split-circle graphic with slash marks will appear under an ultraviolet light.

2 Chip – The card may have a chip. Cards with chips also have a magnetic stripe.

3 Embossed account number – All Diners Club account numbers start with 30, 36, 38 or 39. Embossed card numbers should be uniform in size and spacing.

4 Cardholder name – The card will be embossed with the cardholder name.

5 Expiry dates – 'Valid' and 'Thru' dates indicate the first and last month in which the card is valid.

6 Magnetic stripe – The holographic magnetic stripe contains a repeating image of the logo, name and world map which shift colour and appearance when the card is tilted. It should appear smooth, with no signs of tampering. Some cards may have a standard black magnetic stripe.

7 Signature strip – The Diners Club split circle graphic appears on a tamper-evident signature panel.

8 Account number on signature strip – A full or partial account number may appear in indent printing.

9 Card Security Code – CSC code appears on the signature panel in indent printing.

10 Acceptance marks – Other acceptance marks or logos such as Discover or pulse® may appear on the back of the card.

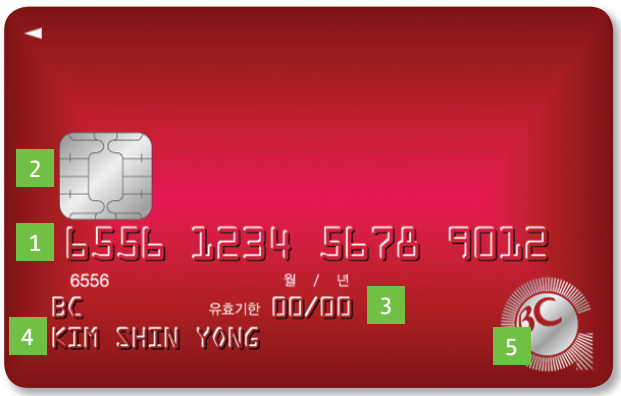
CARDNET HELPLINE

Call 01268 567 100

8am to 9pm Monday to Saturday

Call our knowledgeable UK-based team with any questions about your Cardnet service or this manual.

BC Global Card



These card images are for visual purposes only.

BC Global Card is a partner brand of Discover Financial Services and is the largest domestic network in South Korea. As Korea's biggest credit card company, BC Global Card currently have 11 financial institution partners and have issued approximately 55 million cards in Korea.

1 Embossed account number – The account number appears on the front of the card with the first four digits printed below.

2 Chip – An embedded chip appears on the front of the card.

3 Expiry date – 'Valid Thru' indicates the last month in which the card is valid.

4 Cardholder name – The cardholder name is embossed on the front of the card.

5 BC Global Card logo – The logo appears on the front of the card.

6 Magnetic stripe – The magnetic stripe should appear smooth and straight, with no signs of tampering.

7 Signature strip – The signature panel is shortened on chip-enabled cards. The signature on the card should match the customer's signature on the receipt.

8 Acceptance marks – The back of the card should display the acceptance marks of Discover, Diners Club International and pulse, in addition to the BC Global Card Logo.

DinaCard

7
POTPIS KORISNIKA KARTICE / AUTHORIZED SIGNATURE
8
NE VAŽI BEZ POTPISA / NOT VALID IF NOT SIGNED
This is property of Agrobanka a.d. Beograd, Sremska 3-5 and must be returned upon request. Misuse is a criminal offence. If found, please return to Agrobanka a.d. Belgrade. Customer service 381 11 2623 025
9
10
Diners Club INTERNATIONAL
DISCOVER
pulse
Agrobanka
Agrobanka a.d. Beograd
Sremska 3-5, 11000 Beograd

These card images are for visual purposes only.

DinaCard is a partner brand of Discover Financial Services and is operated by the national Serbian payment card network, which is a division of the National Bank of Serbia, Serbia's central bank, in partnership with a number of issuing banks. The design of the card is unique for each bank. The name of the issuing bank will appear on the front and the back of the card.

1 Chip – The card may have a chip. Chip cards will also have a magnetic stripe.

2 Embossed account number – The account number appears on the front of the card. Embossing should be straight and uniform in appearance.

3 Cardholder name – The cardholder name is embossed on the front of the card.

4 Expiry date – 'Valid Thru' indicates the last month in which the card is valid.

5 DinaCard logo – The DinaCard logo appears on the front of the card.

6 DinaCard hologram – The hologram features Queen Natalija and should reflect the light and appear to move when the card is tilted.

7 Magnetic stripe – The magnetic stripe should appear smooth and straight, with no signs of tampering.

8 Signature strip – The signature on the card should match the customer's signature on the receipt.

9 Acceptance marks – The back of the card should display the acceptance marks of Discover®, Diners Club International® and pulse®.

10 Bank card design – DinaCard is issued by 27 different banks in Serbia. The design of the card is unique for each bank. The name of the issuing bank will appear on the front and the back of the card.

CARDNET HELPLINE

Call 01268 567 100

8am to 9pm Monday to Saturday

Call our knowledgeable UK-based team with any questions about your Cardnet service or this manual.

More choice for your customers

Accept payment from one of the widest ranges of card schemes available.

Contactless technology offers swifter transactions

Call our helpline to find out more.

Contactless

AUTHORISED SIGNATURE – NOT VALID UNLESS SIGNED BELOW
1234 123
0845 3 000 000
Any problems using your card abroad call
+44 1733 347 007
You can use your debit card:
• Abroad on your holiday
• Online for goods and services
• Shopping on the high street
lloydsbank.com

These card images are for visual purposes only.

Contactless enabled cards are now a significant proportion of the UK card population. These cards enable purchases for low value transactions (£20 as of 1 June 2012) to be undertaken by waving the card over a Contactless enabled payment acceptance device. This improves the customer payment experience, speeds up transactions and helps retailers to remove cash and cheques from their business.

As part of the security systems for this type of transaction and to protect both consumers and retailers, on occasion, the Contactless transaction will be disallowed and a prompt for a chip and pin transaction will be made. This is a normal action which has been built into the system by the Card Schemes. You will recognise a Contactless enabled card as it will carry the Contactless logo (see left).

Payments using mobile phones and FOBs

Contactless technology is constantly evolving and there are now an increasing number of prepaid Contactless devices available such as mobile phones and FOBs. These work in the same way as a card by waving the phone or FOB over a contactless enabled payment acceptance device.

If you want the option to take Contactless transactions your point of sale equipment will need to be enabled to accept these cards and you will also be required to promote acceptance by displaying the correct acceptance marks. **These are available by contacting the Cardnet Helpline on 01268 567 100.**

Commercial cards

Commercial cards bring specific benefits to a business-to business sales transaction. They look like any other Visa or MasterCard card although many have the description of the card's function on the front of the card. For example, 'Purchasing Card'.

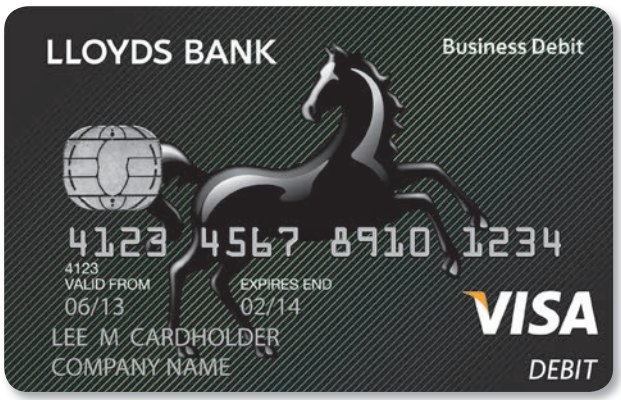
There are three main types of Commercial cards:

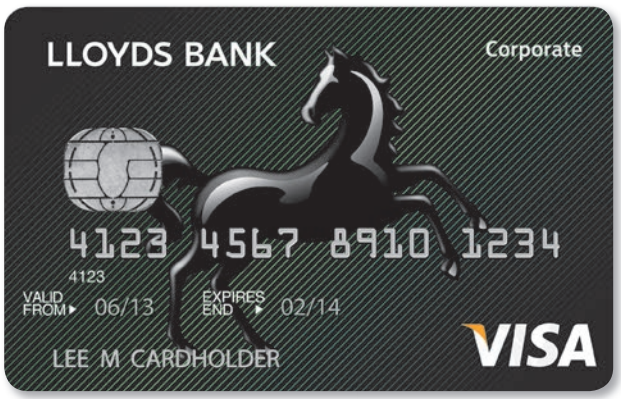
Business card

- Suitable for paying everything a small business needs (e.g. stationery, office supplies, travel and entertainment etc.).
- Provides small businesses with a business payment method, an expense control mechanism and a cash management tool.
- Available as charge and credit cards.

Corporate card

- For travel and entertainment for mid-sized to large companies.
- Provides management information which makes it easier to control expenditure and to manage business expenses.
- Allows streamlined administration of expenses, saving time and money by reducing cash handling and paper-based payment methods.





These card images are for visual purposes only.

Purchasing card

Purchasing cards can be used to settle transactions in the normal way, however, they can also automate the paper invoice system and satisfy VAT reporting requirements.

- Used by Government departments, public sector bodies and large businesses.
- Enables control and monitoring of expenditure and the provision of data and information to help improve cost management.
- Allows VAT reclamation.
- Removes paper-based processes, through electronic invoicing with detailed breakdowns of expenditure.

BENEFITS

In order to capture the full benefits of purchasing cards you will need to upgrade your point of sale equipment. For more detailed information or operating instructions contact the Cardnet Helpline on **01268 567100**

These card images are for visual purposes only.

3 : Checking the card

The following details need to be checked carefully on all cards, even if the holder is well known to you or is a regular customer.

The name of the card (e.g. Visa/MasterCard®/Maestro®, Diners Club International®, Discover®, BC Global card and DinaCard) and card issuer (for example, Lloyds Bank) should appear in bold letters on the card. You should also check the following:

Security features

Front of card

1 Microchip.

2 Card number.

3 Bank Identification Number (BIN).

4 Validity date.

5 Cardholder's name/title.

These card images are for visual purposes only.

Back of card

6 The hologram – the hologram may appear on the front or the back of the card depending on the card type. On this example the hologram appears on the back.

7 Magnetic stripe.

8 Tamper evident signature strip which must be signed.

9 Last four digits of the card number (some older cards in circulation may show the whole account number).

10 Card Security Code.

11 Contactless function.

These card images are for visual purposes only.

The number embossed on the front of the card may be 12 to 19 digits in length dependent on the type of card presented.

This number is tied to the information encoded in the chip, on the magnetic stripe and the number indent-printed on the signature strip. This enables card issuers and sales staff to immediately recognise a counterfeit card when these codes do not match. This makes it more difficult to alter encoded information.

The easiest way to check for inconsistencies in this information is to make sure that the last four digits of the card number embossed on the front of the card match the last four digits electronically printed on the terminal receipt.

Card Security Codes (CSC)

The three-digit CSC may appear on the signature strip next to the full card number (or alternatively the last four digits from the card number), or it may appear in a white box beside the signature strip. These additional digits are a further security feature for use in 'Card Not Present' (CNP) transactions. (See Section 4, 'Accepting transactions' p39.)

Tamper-evident signature strip

The signature strip on most cards has a feature whereby the strip will change colour if the signature is tampered with.

Indent printing

The last four digits of the card number, together with the three-digit CSC, are printed using a unique reverse italic font on the signature strip on the back of the card which makes alteration extremely difficult. The four digits should match the last four digits of the card number on the front of the card. Some older cards in circulation may show the whole account number followed by the three-digit CSC.

UV (ultraviolet) lamp test

You may already use a UV lamp to check for fake bank notes. Cards can also be checked in the same way. If you place a genuine card under a UV lamp you should see a special mark. If these features do not show, the card is probably a counterfeit. In these circumstances you should make a Code 10 call to the Authorisation Centre, see Section 7, 'Security, Suspicious transactions'.

Visa UV image

Older cards will still show the dove image in the centre of the card. Please be aware that some Electron cards do not have a UV image.

Newer Visa cards will show an ultraviolet 'V' over the Visa brand mark.

MasterCard UV image

MasterCards will show the letters 'MC'.

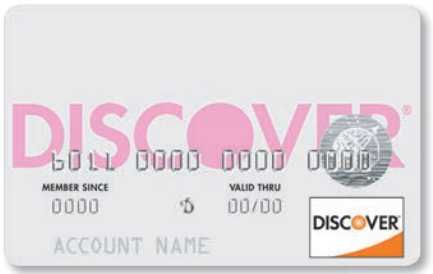
These card images are for visual purposes only.

Maestro UV image

The word Maestro will show on the front of the card in the bottom left-hand corner.

Discover Card UV image

'DISCOVER' or 'DISCOVER NETWORK' will appear across the middle of the card under an ultraviolet light.



Diners Card International UV image

The Diners Club split circle graphic in an invisible line pattern will appear in the middle of the card in blue cast fluorescent ink.

BC Global Card UV image

The letters 'BC' will appear on the front of the card under an ultraviolet light.

DinaCard UV image

DinaCards do not have a UV image.

These card images are for visual purposes only.

Hologram

Check the hologram which appears on the face or reverse of all Visa, MasterCard®, Maestro®, Diners Club International®, Discover® and DinaCard cards.

The holograms to look for are:

- Visa and Visa Electron – a flying dove which moves and changes colour when tilted.
- MasterCard – two interlocking globes which change colour when tilted.
- UK Maestro – Maestro logo.
- Diners Club International – most cards carry a holographic magnetic stripe containing a repeating image of the logo, Diners Club International name and world map which shift colour and appearance when the card is tilted. It should appear smooth, with no signs of tampering. Some cards may have a standard black magnetic stripe.
- Discover – all cards display a hologram on the front of the card with a globe pierced by an arrow, unless the back of the card displays a holographic magnetic stripe.
- BC Global Card – BC Global cards do not have a hologram.
- DinaCard – The hologram features Queen Natalija and should reflect the light and appear to move when the card is tilted.

CARDNET HELPLINE

Call 01268 567 100

8am – 9pm Monday – Saturday

Call our knowledgeable UK-based team with any questions about your Cardnet service or this manual.

Additional checks

The following additional checks will help you validate the cards handed to you when carrying out over the counter transactions.

1 Validity dates: The majority of cards will have effective (valid from) and expiry (valid to) dates which are located on the face of the card. The transaction date must fall on or between these dates. Do not accept a card prior to the effective date (the first day of the month) or after the expiry date (up to and including the last day of the month) or you may be subject to a chargeback. Some cards may just have an expiry date. In these cases you'll need to make sure that transactions are not accepted after the last day of the month of expiry.

   Please note that some V PAY cards may not have either a valid from or expiry date.

2 Cardholder's title: If the cardholder's title is embossed on the front of the card (for example, Mr, Mrs) check that it is appropriate to the person presenting the card. Check that there is no obvious discrepancy between the cardholder and the card.

3 Cardholder's signature: The signature strip should not be disfigured or tampered with in any way and should have only one signature. If you are presented with an unsigned card, please contact the Authorisation Centre immediately for advice, stating "This is a Code 10 authorisation" – see Section 7, 'Security, Suspicious transactions'. Do not allow the cardholder to sign the card until you have received instructions from the Authorisation Centre. If the card is a chip and PIN card and the cardholder has successfully entered the PIN, they should be advised to sign the card.

4 Bank Identification Number (BIN): On Visa and MasterCard cards check that the first four digits of the card number are printed in small characters below the first four digits of the card number. If the four digits are missing or do not match, the card is probably counterfeit.

5 Damaged cards: Ensure that the chip or magnetic stripe on the card you are presented with has not been mutilated or damaged in any way.

Code 10

If after making these checks you think the card may be invalid, keep the card and do not release the goods or provide the services. Telephone the Authorisation Centre immediately, stating "This is a Code 10 authorisation" – see Section 7, 'Security, Suspicious transactions'.

Reward

A reward of £50 will normally be paid to any Cardnet merchant who recovers a card, when requested to do so by the Authorisation Centre.

Please note: Discover Financial Services do not participate in the Reward scheme. This means we are unable to pay a reward for the recovery of Diners Club International®, Discover®, BCcard or DinaCard cards.

4 : Accepting transactions

This section explains how to conduct the various types of transaction smoothly and securely.

Cardnet allows your business to accept over-the-counter transactions and, with our written agreement, telephone or mail orders using certain types of card. You can also accept Internet payments by applying to Cardnet for an E-commerce facility.

Over-the-counter transactions

All transactions must be processed through an electronic terminal.

Always follow the instructions shown in the user manual supplied with your terminal.

Below is a brief summary of the procedures you need to follow when processing card transactions.

Chip and PIN card transactions

1 Ensure the card is inserted into the card reader.

2 Follow your terminal operating instructions.

3 The cardholder will be prompted to enter their PIN.

What if the cardholder enters an incorrect PIN?

The cardholder has three chances to enter their PIN. If on the third attempt the PIN is entered incorrectly the PIN number will lock. At this stage you should tell the cardholder that their PIN has locked and ask for an alternative method of payment.

Contactless receipt.

WHITES OF LONDON
LONDON SW 5
599999999999999
TID36144293
AID : A0000000031010
VISA CREDIT
VISA
XXXX XXXX XXXX 0019
EXP 12/14
CONTACTLESS
MERCHANT COPY
AMOUNT £5.00
09:45 27/11/09
AUTH CODE: 06544
RECEIPT 0154

Verified by PIN receipt.

WHITES OF LONDON
LONDON SW 5
599999999999999
TID36463725
AID : A0000000041010
MasterCard
MASTERCARD
XXXX XXXX XXXX 0020
EXP 12/09 START 01/04
ICC PAN.SEQ 00
SALE
MERCHANT COPY
AMOUNT £10.00
GRATUITY £0.00
TOTAL £10.00
Verified by PIN
PLEASE DEBIT MY ACCOUNT
09:32 13/10/09
AUTH CODE: 006539
RECEIPT 0038

Chip card transactions

1 Insert the card into the card reader.

2 Follow your terminal operating instructions.

3 Ask the cardholder to sign the receipt.

Please be aware that some chip cardholders may still have chosen to identify themselves with a signature rather than a PIN. In these circumstances please check the card following the instructions in Section 3, 'Checking the card' (p33).

Accepting Contactless card payments

1 The cardholder simply waves their card, FOB, mobile phone or other device over the Contactless reader.

2 Transaction complete.

Sales – a single Contactless transaction is permitted only for an amount under a predefined limit set by the Card Schemes. We will notify you of the current limit and let you know if there is any change to this limit. Transactions above the 'Contactless' limit must be processed following your terminal prompts.

Refunds – all refunds should be processed following your terminal prompts.

Any transaction that is not able to be processed as a Contactless transaction should be processed following your terminal prompts.

There will be occasions where it will be necessary for additional security checks to be carried out on Contactless cards which will require the sale to be a full chip and PIN transaction. Cardholders will be aware of this.

Receipts – cardholder copies of receipts are optional.

Important

If a chip and PIN card is presented and for any reason you process the transaction without a PIN being entered, you may be liable for any chargebacks.

Magnetic stripe only card transactions

Most UK cards are issued with chip and PIN; however, some cards will continue to be issued without a chip and will be read by the magnetic stripe. This also tends to be the case for some cards issued outside Europe. Please examine these cards carefully.

1 Check the card: Follow the step-by-step instructions in Section 3, 'Checking the card' (p33). Only when you are satisfied with all checks, should you proceed.

2 Swipe the card: Refer to the procedures in your terminal operating instructions. As an extra security measure you may be prompted to key enter the last four digits of the number embossed on the front of the card. The terminal will then check these numbers against those held in the card's magnetic stripe.

3 Authorisation: All transactions must be authorised. Refer to Section 5, 'Authorisation and referrals' (p55).

4 Signature: Ask the cardholder to sign the receipt and check that the signature matches that on the reverse of the card.

5 Check the receipt: Compare the card number printed on the receipt with the number embossed on the front of the card – see Section 3, 'Checking the card'. If the numbers do not match, telephone the Authorisation Centre immediately for advice, stating "This is a Code 10 authorisation" – see Section 7, 'Security, Suspicious transactions' (p73).

You must retain copies of all sales and refund receipts for a minimum of 13 months. This will assist you in checking your statements and resolving any possible chargebacks. Please see Section 7, 'Security' (p65) for details on how this information must be stored. If you are unable to produce a copy, the transaction may be charged back to you.

6 Return the card: Once you have completed all the above steps, return the card to the cardholder together with any goods purchased and a signed copy of the receipt.

Mag-stripe receipt.

WHITES OF LONDON
LONDON NW 5
5999999999999999
TID36463725
MASTERCARD
XXXX XXXX XXXX 0608
EXP 12/10
SWIPED
SALE
MERCHANT COPY
AMOUNT £10.00
GRATUITY £0.00
TOTAL £10.00
PLEASE DEBIT MY ACCOUNT
Thank You
09:34 13/10/09
AUTH CODE: 006540
RECEIPT 0039

Card Not Present (CNP) transactions

Provided you have received written agreement from Cardnet you may accept a telephone or mail order from a cardholder who wishes to pay using a Visa, MasterCard, Maestro, Discover Financial Services or partner card.

You must not accept internationally issued Maestro cards and V PAY for CNP transactions. Visa Electron cards can be accepted for CNP, as long as transactions are always authorised.

When accepting a CNP order, please take extra care to ensure you have permission to debit the card account and it is the genuine cardholder who placed the order as you are responsible for any transactions where the card and the cardholder are not present.

The following examples are all acceptable as CNP orders.

Mail orders – written authority from the cardholder, bearing the cardholder's signature in any form including:

- Completed order forms.
- Facsimile transmissions.

If you conduct CNP transactions by mail, the cardholder's signature must appear on your order form. You must also keep the instruction for 13 months in case the transaction is disputed at a later date.

Telephone orders – authority from the cardholder by telephone.

When taking an order by telephone always record in writing all details of the transaction along with time and date of the conversation as you may be asked to produce this or the cardholder's authority for a CNP sale if the transaction is disputed at a later date.

For all orders received by mail, telephone or fax, goods must be delivered and it is advisable to keep documentary evidence of the delivery address for 13 months.

If you are unable to deliver the goods immediately, your authorisation is only valid for seven calendar days.

All mail/telephone order transaction records must be kept securely. Full details about how to store cardholder information can be found in Section 7, 'Security'.

Collecting cardholder information for CNP transactions

When a cardholder is not present for the sale, you must obtain the following information in order to verify their identity and help validate the transaction:

- Card number.
- Card expiry date.
- Card issue number, if present on the card.
- Cardholder name and initials as shown on the card.
- The Card Security Code (CSC) (the three-digit number on or near to the signature strip on the back of the card, or on American Express cards the four-digit number on the front of the card).
- The address known to the cardholder's bank (for example, where their card statements are sent to).
- Contact telephone number (it is a higher risk to accept a mobile telephone number).

This information will enable you to carry out the usual status check so that you can confirm whether the cardholder has sufficient funds to pay you. It also allows you to find out whether or not the card has been reported lost or stolen.

You will be asked to produce this information, except for the CSC, if the transaction is disputed at a later date.

Important

Under no circumstances can goods paid by mail or telephone be handed over the counter to, or collected by, the cardholder. See Section 7, 'Security, How to guard against fraud' (p75).

If a cardholder wishes to collect the goods, then they must attend your premises in person and produce their card. Any Sales Voucher already prepared must be destroyed and an over the counter transaction processed. If you have already completed a CNP order you must either cancel the transaction or perform a refund. If you perform a refund, please let the cardholder know that the original transaction, a refund and the over the counter transaction will all appear on their card statement.

If authorisation was obtained for the original transaction, or your terminal indicates that manual authorisation is required, you must telephone the Authorisation Centre.

The Address Verification Service (AVS) and Card Security Code (CSC)

Since the introduction of chip and PIN fraudsters have increased their activity in Card Not Present transactions.

As you are responsible for any transactions where the card and the cardholder are not present, as well as collecting the Card Security Code (CSC), we recommend you complete these transactions using the Address Verification Service.

What are the Address Verification Service and Card Security Code?

The Address Verification Service (AVS) is available on all UK issued cards, with the exception of Discover Financial Services and partner cards, and allows you to check the numerical part of the cardholder's postcode and statement address with the card issuing bank.

1 Card Security Code (CSC) – The three-digit security code may appear on the signature strip next to the full card number (or alternatively the last four digits from the card) or it may appear in a white box beside the signature strip.

Please remember you remain ultimately responsible should a transaction be confirmed as invalid or fraudulent, even if the AVS and CSC data matches and an authorisation code is given.

Collecting the Card Security Code and Address Verification information

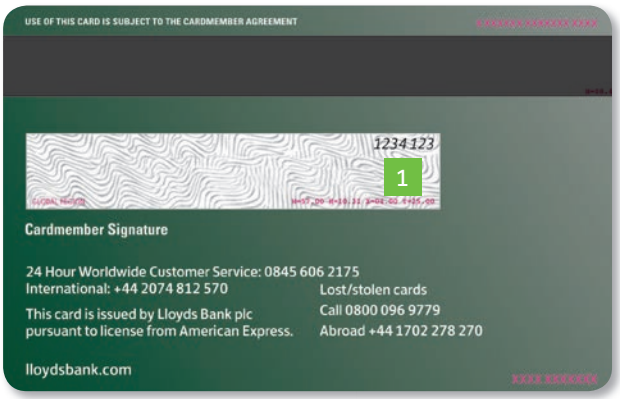
You must always ask the cardholder for their Card Security Code as this is a good indication that they have the card in their possession when they are ordering from you.

On the majority of cards, only the last four digits of the card number are repeated in the signature strip, followed by the three-digit CSC.

2 For American Express cards the CSC is a four-digit number and it appears on the front of the card.

Please remember that you must not retain the CSC after the transaction has been authorised.

Please note you can verify the CSC on Discover and Diners Club International cards. However, the AVS is not supported on these cards.


USE OF THIS CARD IS SUBJECT TO THE CARDMEMBER AGREEMENT
1234 123
1
Cardmember Signature
24 Hour Worldwide Customer Service: 0845 606 2175
International: +44 2074 812 570
Lost/stolen cards
Call 0800 096 9779
This card is issued by Lloyds Bank plc pursuant to license from American Express.
Abroad +44 1702 278 270
lloydsbank.com

These card images are for visual purposes only.

Address Verification Service

Because criminals can use lost or stolen cards to order goods in CNP situations, it is possible that they might be able to give you the CSC. However, it is less likely that a fraudster would also have the cardholder's address, so the AVS will act as an additional check.

The AVS is available on all UK issued cards, with the exception of Discover Financial Services and partner cards, and allows you to check the numerical part of the cardholder's postcode and statement address with the card-issuing bank.

You will need to ask the cardholder for their address as recorded by their card-issuing bank and input the relevant numbers as shown in the examples below.

Cardholder's details to be entered:

Cardholder's address	Card Security Code	Post Code Numeric	Address numerics*	Details to be entered when prompted by your terminal
20 High Street Any Town Any County TN26 2BN	123 or 7594	262	20	12326220 or 759426220
Flat 1A 25 London Road Any Town Any County BN4 6RJ	123 or 7594	46	125	12346125 or 759446125
Rose Cottage Mill Lane Any Town Any County SS21 3HP	123 or 7594	213		123213 or 7594213
Flat 12A 1067 Main Road Any Town Any County RG12 4UB	123 or 7594	124	12106	12312412106 or 759412412106
			*Maximum five digits (if over five, take first five digits).	

When using an electronic terminal enabled with the AVS functionality to process CNP transactions, your terminal will automatically prompt for the AVS information and call the Authorisation Centre as normal. Transactions should take the same time to authorise, even though you have given us more information to check.

The CSC and AVS are designed to eliminate the need for CNP Code 10 calls, this means the Authorisation Centre cannot be used for any additional checking. This is because the Authorisation Centre will only be able to perform the same checks as your terminal and you will also run the risk of receiving two authorisation numbers for the same transaction.

Please note: You can verify the CSC on Discover and Diners Club International cards. However, the AVS is not supported on these cards.

Your customers should now be used to giving the additional information for CNP transactions. The protection against card fraud is a benefit to them as well as to you and should be used. These extra security measures shouldn't make any difference to the speed it takes to authorise a transaction electronically. In fact, authorisation could be quicker because you will no longer need to make CNP Code 10 phone calls. Plus, the final decision on whether or not to accept a payment is still up to you.

Authorisation responses

If there are available funds and the card hasn't been reported lost or stolen, you will receive one of the standard responses shown in the table below.

It is your decision whether or not you wish to progress a CNP transaction, and this additional information will help you decide. However, as with all CNP transactions, payment is not guaranteed and you bear the risk if the transaction is disputed at a later date.

Response	Definition	Preferred actions
Data Matches	This means that both the AVS and CSC match the card-issuing bank's records.	As long as you have been given an authorisation code, and you are satisfied that the transaction is genuine, then unless there are other suspicious circumstances that concern you, you may decide to go ahead with this sale. However, as with all CNP transactions, payment is not guaranteed and you bear the risk if the transaction is disputed at a later date.
Data Non Match	The CSC and/or the address details don't match with the card-issuing bank's records.	Your terminal may decline your transaction. There is the possibility that this is a fraudulent transaction. Further enquiries with the cardholder should be made. It could also be that the member of staff has noted the details incorrectly, so you may want to check your records.
CSC Match Only	Only the CSC matches and either one or both of the address details don't match with the card-issuing bank's records.	The address given must match the address recorded by the card-issuing bank, so in this case there is a possibility that the transaction is fraudulent. However, it could also mean that the cardholder has changed address without notifying the card-issuing bank or the card-issuing bank doesn't support AVS. Another possibility is that a member of staff may have noted the details incorrectly. In these circumstances it would be advisable to verify the address again with the cardholder and for you to check your records.
AVS Match Only	Both address and postcode match, or just the postcode in cases where the home address has a house name rather than a number. However, the CSC doesn't match.	Your terminal may decline your transaction. There is the possibility that this is a fraudulent transaction. However, it could be that the cardholder has given you an incorrect CSC number by mistake. It could also be that a member of staff has noted the number down incorrectly. Therefore, before taking any further action, you may want to verify the CSC again with the cardholder. You may also want to check your records.
Not Checked	This means that neither the CSC nor the AVS has been checked.	This could be because the card-issuing bank doesn't support either of the services, or their system is down. If this happens then you will have to make a decision based on the information you have, as you do now. We would recommend that you make further checks before going ahead with the sale.

Next steps

- If a transaction has been authorised, but you are not happy to continue, you should process a reversal or refund immediately to reinstate available credit to the cardholder.
- If the transaction is referred, the CSC and AVS information may be returned by your terminal so that you can verify the transaction with the Authorisation Centre by telephone: CNP Authorisation **01268 278 278.**

Important information

Please read the points detailed below. These points explain a few key things that you should be aware of when processing CNP transactions.

This information should answer some of the questions you may have about the processes, but if you have further queries, please call the Cardnet Helpline on **01268 567 100.**

1 Guidance only

Please remember the use of CSC checks and AVS is not a guarantee of payment. They are there to help you establish if the card is present at the time of the transaction and that you are more likely to be dealing with the genuine cardholder.

2 Transaction approval criteria

The CSC and AVS checks are in addition to the overall card status check. The overriding criteria are still the availability of funds and card status.

3 Delivery address

If you deliver goods to a different address, other than the one checked using the AVS service, you are taking an additional risk.

4 Destroying records

If you keep records of your transactions in any format other than the Cardnet Mail Order Transaction schedule, you must ensure that you do not keep any records of cardholders' Card Security Codes. This information must be destroyed once the transaction has been authorised.

5 Overall responsibility

It is your decision whether or not you wish to progress a CNP transaction, and this additional information will help you decide. However, please remember that you remain ultimately responsible should a transaction be confirmed as invalid.

6 Declined transactions

Even if the CSC and AVS data matches, never process a declined transaction.

E-commerce

If you wish to trade over the Internet and take payments from debit and credit card holders for your goods or services, you will need a separate merchant account and Cardnet's prior agreement to accept cards in this way. A new application must be made for an E-commerce facility with Cardnet even if you have an existing Cardnet facility for over the counter or mail order/telephone order transactions.

When your E-commerce account is approved, you will be issued with a new Cardnet merchant number. This number must be used for E-commerce sales only. The reason for this is that all E-commerce transactions must be identified separately.

Your website must contain all of the following information:

- Card Scheme logos in full colour to indicate card acceptance.
- Complete description of the goods or services offered for sale by you on your website and any return/refund policy.
- Customer service contact, including electronic mail address or telephone number and international dialling code.
- Your business address and country.
- Transaction currency.
- Export restrictions (if known).
- Delivery policy.
- Consumer data privacy policy.
- Security capabilities and policy for transmission of payment card details.
- Cookie policy and data protection policy.
- Your purchase terms and conditions made available to the cardholder during the order process, either:
  - on the same screen used as the checkout screen indicating the total transaction amount; or
  - within the sequence of web pages accessed by the cardholder prior to the final checkout.

Cardholder receipts

Your customers must be supplied with a transaction receipt (this must be part of an order confirmation notice) at the time of the purchase. Please remember, the receipt must not include the full card number.

Processing E-commerce transactions

To process E-commerce transactions you will need to use a Payment Service Provider (PSP), which must be approved by Cardnet. Your chosen PSP will be able to advise you of relevant costs, set-up times and how their systems integrate with your website. To see a list of the PSPs we currently work with you can contact the Cardnet Helpline on **01268 567 100** or go to the useful links and services page on **lloydsbankcardnet.com**

We would strongly recommend that you use a fully 'hosted' solution provided by your chosen PSP. In simple terms this means having the payment application (cardholder payment page) hosted on the PSP's secure servers. If you choose the secure hosted option, the Payment Card Industry Data Security Standard (PCI DSS) validation requirements for E-commerce merchants are greatly reduced.

PCI DSS is a set of requirements, endorsed by the Card Schemes (Visa, MasterCard and Discover Financial Services) governing the safekeeping of account information and applies to anyone that stores, processes or transmits cardholder data.

To see how PCI DSS affects you as an E-commerce merchant and what you need to do to validate your compliance with these standards – see Section 7, 'Security, Data security' (p66).

Verified by Visa, MasterCard SecureCode and Diners Club International ProtectBuy.

Verified by Visa, MasterCard SecureCode and Diners Club International ProtectBuy are industry-wide initiatives introduced to combat fraud over the Internet. Much like chip and PIN for 'over-the-counter' transactions, cardholders who register for these services will be required to input an individual PIN or password at the time of the transaction to confirm they are the genuine cardholder.

All Maestro E-commerce transactions must be authenticated with MasterCard SecureCode according to current Card Scheme regulations.

How do Verified by Visa, MasterCard SecureCode and Diners Club International ProtectBuy work?

Verified by Visa, MasterCard SecureCode and Diners Club International ProtectBuy operate on your website and interact with both the cardholder and their card issuer.

The cardholder signs up for these extra security features with their card issuer.

When shopping online:

1 The cardholder selects their chosen goods and proceeds to the payment page.

2 The cardholder enters their card number. If they are registered for Verified by Visa, MasterCard SecureCode or Diners Club International ProtectBuy, a pop-up or in line screen from their card issuer appears asking for their password (or random characters as set out by their card issuer's authentication requirements).

3 The card issuer verifies the password.

4 The transaction is completed giving both the merchant and the cardholder the confidence that the identity of each has been verified.

Please note: Some UK card issuers will assess each transaction and verify them automatically. Instead of being asked to input a password or random set of characters, cardholders will receive a message in a pop-up or in line screen to confirm that the transaction is being processed.

These services also benefit merchants. By deploying Verified by Visa, MasterCard SecureCode and Diners Club International ProtectBuy you will be protected from most chargebacks where the cardholder subsequently denies engaging in or authorising the original transaction.

For more information on Verified by Visa, MasterCard SecureCode and Diners Club International ProtectBuy, contact the Cardnet Helpline on **01268 567 100.** Lines are open 8am–9pm, Monday to Saturday.

Alternatively, for merchant and consumer advice, frequently asked questions (FAQs) and online demonstrations on how these solutions work, visit:

www.visaeurope.com (Businesses and Retailers)

www.mastercardmerchant.com/securecode

www.dinersclubinternationalprotectbuy.com

www.financialfraudaction.org.uk

Card Schemes

Your Cardnet facility allows you to accept many different types of cards. The guide below shows you the processing options possible for each of the different Card Schemes.

Card type	Electronic processing	Manual key entry	Mail and telephone order*	E-commerce*	Purchase with Cashback*
MasterCard	✔	✔	✔	✔	✘
Debit MasterCard	✔	✔	✔	✔	✔
Maestro	✔	✔	✔	✔#	✔
International Maestro	✔	✘	✘	✔#	✔
Visa Credit	✔	✔	✔	✔	✘
Visa Debit	✔	✔	✔	✔	✔
Electron	✔	✘	✔	✔	✔
V PAY	✔	✘	✘	✔**	✔†
Discover	✔	✔	✔	✔	✘
Diners Club International	✔	✔	✔	✔	✘
BC Global Card	✔	✔	✔	✔	✘
DinaCard	✔	✔	✔	✔	✘
Corporate, Commercial and Purchasing cards	✔	✔	✔	✔	✘

* The acceptance of these facilities must also be agreed with Cardnet. For more information contact the Cardnet Helpline on **01268 567 100.** Lines are open 8am–9pm, Monday to Saturday.

Maestro cards can only be accepted over the Internet if you are registered for MasterCard SecureCode. For more information about MasterCard SecureCode see, Section 4 'Accepting transactions' pages p51 and p52, or visit **www.mastercardmerchant.com/securecode**

† If permitted by the issuer.

** V PAY can only be accepted over the Internet if:

- Permitted by the issuer.
- You are registered for Verified by Visa.

For more information about Verified by Visa see pages p51 and p52, Section 4 'Accepting transactions', or visit the Business and Retailers Section of **www.visaeurope.com**

For more information about Diners Club International ProtectBuy see pages p51 and p52, Section 4 'Accepting transactions', or visit **www.dinersclubinternationalprotectbuy.com**

Please note that zero floor limits will apply to all of the following transaction types below and you must always obtain an authorisation for such transactions.

Where the customer is present:

- All magnetic stripe read transactions.
- All key entered transactions.
- All paper or manually processed transactions (authorisation by telephone).
- All purchase with cashback transactions.

Where the customer is not present:

- All Card Not Present transactions which include Mail/Telephone Order, E-commerce (Internet) and Recurring transactions.

Please remember that if you process any of the above transactions without authorisation they may be rejected by the card issuing bank and charged back to you.

5 : Authorisation and referrals

This section explains when authorisation is required for transactions and how to conduct a referral. It also covers the processes for splitting sales with other payment types, cancelling a transaction and providing a refund.

When to obtain authorisation

Authorisation must be obtained (in accordance with your terminal operating instructions and your Retailer Agreement) before the sale is concluded.

Your terminal will, in most cases, obtain authorisation for transactions equal to or over your floor limit. However, it is your responsibility to ensure that all the relevant checks are carried out – see Section 3, 'Checking the card' (p33).

Manual authorisation

You must manually authorise the transaction if:

- Your terminal indicates that it is necessary to do so. You must make an authorisation call and let the Authorisation Centre know that you are calling as a result of a terminal referral.
- You are using the paper fallback procedures – see Section 9, 'Exceptions' (p93).
- There is a split sale – see page p57 in this section.
- You are suspicious of a card/cardholder – in these circumstances a 'Code 10' authorisation should be made – see Section 7, 'Security, Suspicious transactions' (p73).

Remember: authorisation is not a guarantee of payment. It confirms that the card has not been reported lost or stolen at the time of the transaction and that adequate funds are available.

Authorisation adjustments/reversals

If there is any change in the authorised amount of the sale, or if the sale is cancelled or a refund issued, please contact the Authorisation Centre stating you wish to cancel or amend an authorisation.

You will be asked to provide:

- The card number.
- Your Cardnet merchant number.
- The amount of the original authorisation.
- The card expiry date.
- The issue number of the card (if applicable).
- The original authorisation code.

Referrals

Occasionally your terminal may request that you call the Authorisation Centre. If this happens, call the Authorisation Centre on the telephone numbers detailed on page p58 as the card issuer may have grounds to suspect that the transaction could be fraudulent.

The card issuer may ask you to relay some simple cardholder identification questions or ask to speak to the cardholder direct. If this happens please make sure that you take the telephone back from the cardholder before the call is terminated so that you can check that the issuer is happy for the transaction to proceed. The issuer will then give you an authorisation code to enter into the terminal. You must ensure that you only accept the authorisation code from the operator, otherwise you could be liable if the transaction is disputed at a later date. Any transactions processed with an invalid authorisation code may be charged back to you.

Referrals can occur for a number of reasons, for example, high value transactions.

However, they do not necessarily reflect on the creditworthiness of the cardholder.

Split sales with cash, cheque or second credit card

If the total price for goods or services is equal to or exceeds your floor limit and payment is offered partly by MasterCard or Visa and partly by cheque, cash or any other method, authorisation must be obtained for any part of the transaction being paid for by card – even if the card amount is below your floor limit. The Authorisation Centre must be informed that the request for authorisation is in respect of a split sale. They may require further details.

A single card transaction should never be completed as two or more transactions on the same card, as there is a high risk that you will receive a chargeback for these split sales.

If you have any questions or require guidance in relation to authorisation issues, please ensure that enquiries are directed to the Cardnet Helpline on **01268 567 100** and not your local branch manager.

Cancelling a transaction

If a transaction has been processed in error or the transaction amount changes you must, wherever possible, cancel the transaction.

1 Cancel the transaction: refer to the procedures in your terminal operating instructions.

2 Receipt: give the cardholder a copy of the cancelled receipt.

3 Cardholder's available credit: let the cardholder know that they may need to contact their card issuer as the cancellation could affect their available credit.

Refunds

1 If you wish to provide a refund, the refund transaction must be completed using the same card as the one used for the original sale.

2 You may only process refunds in respect of original sales. Failure to observe this could lead to settlement funds being withheld pending further investigation by us.

3 You must not make a refund to a card where the original sale was made by cash or cheque.

4 You should verify the cardholder (for the refund) in the same way you did for the sale.

5 If your terminal indicates that a manual authorisation is required, you must telephone the Authorisation Centre.

6 You may only perform a refund agreed on the telephone or in correspondence if you manually key enter transactions. Please follow the manual key entry procedures in your terminal operating manual.

7 For over the counter transactions you must enter the card into the chip card reader or swipe it. If the terminal cannot read the card, refer to the failed transactions procedures in Section 9, 'Exceptions'.

8 You must sign the terminal sales receipt, and make a note of the exchange and/or return of any items.

Remember: authorisation is not a guarantee of payment. It confirms that the card has not been reported lost or stolen at the time of the transaction and that adequate funds are available.

FOR AUTHORISATION PLEASE TELEPHONE

01268 822 822
Over the counter (OTC)

01268 278 278
Card not present (CNP)

Lines are open 24 hours a day, seven days a week.

6 : Banking and reconciliation

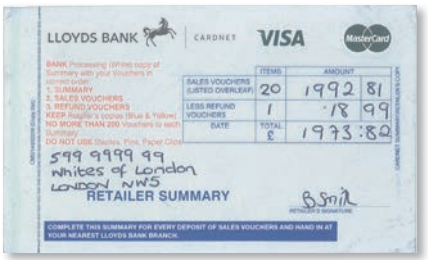
Information on submitting electronic and paper data, record keeping, your Cardnet paper statement and the online reporting tool.

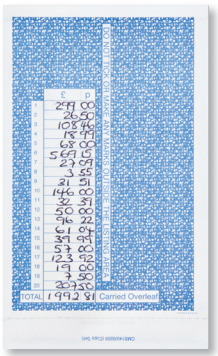
Electronic data

All electronic data sent to us must be in the correct format (any equipment approved by us will be in the correct format). If you use your own equipment or if you would like further information, please request a copy of the Electronic Submissions Guide by calling the Cardnet Helpline on **01268 567 100.**

Make sure that you complete your end of day banking procedures and submit your transactions at agreed times to ensure you receive prompt payment for all card transactions.

For details of agreed times contact the Cardnet Helpline on **01268 567 100.** The Cardnet Helpline will be able to give merchants details of their timescales.





Paper vouchers (for transactions accepted when your terminal is not working)

Preparing over the counter sales and Refund Vouchers for processing*

The Retailer Summary Voucher comes in three parts. The yellow and blue parts are the merchant's copies and the white part is the processing copy, which you need to send to us for processing.

You must take the following steps:

1. Complete a Retailer Summary Voucher with a ballpoint pen.
2. List the amount of each Sales Voucher and the total in the spaces provided on the back of the Retailer Summary Voucher.
3. Prepare a separate listing if there is insufficient space on the summary.
4. Please do not use staples, pins or paperclips.
5. Do not batch more than 200 vouchers on one summary.
6. Complete the front of the summary set (the retailer copy) as follows:
   - Enter the total number of Sales Vouchers and total amount.
   - Enter the total number of Refund Vouchers and the total amount.
   - Enter the net total amount by deducting refunds from sales.

7 Detach the bottom copy and assemble the documents in the following order:
   - Retailer Summary (processing copy).
   - Separate listing, if used.
   - Sales Vouchers (in the same order as listing).
   - Refund Vouchers.
8 Place in the envelope provided for submitting paper vouchers to Cardnet.
9 Retain the two top (yellow and blue) retailer copies of the Summary Voucher and keep with your copy of the Sales Vouchers.

*Paper transactions are not permitted for Discover Financial Services cards or partner cards on over the counter transactions.

Preparing your Card Not Present Transaction Schedules for processing

Each Retailer Summary Voucher completed will result in a separate credit entry to your bank account. Your bank account will be credited once the vouchers have been processed by us. If the value of refunds is equal to the value of Sales Vouchers, then no credit will be made to your bank account.

If you have insufficient Sales Vouchers against which to offset the Refund Voucher(s), complete a Retailer Summary (see page p60) and enter the details of the refund(s).

The value of the refund(s) should be enclosed by brackets, preceded by a minus sign to clearly indicate that the total is a negative value.

The Retailer Summary Voucher and the corresponding Refund Voucher(s) should be sent to Cardnet at the address detailed on page p62.

The value of refunds will subsequently be debited from your bank account.

It is important that you submit the vouchers within the timescales given. If you do not, the transactions may be rejected by the card issuers (even though the proper authorisation procedures have been followed).

You must retain copies of all Summaries, Sales and Refund Vouchers for at least 13 months. This will assist you in checking your statement and resolving any possible chargebacks. If you are unable to produce a copy of the relevant Summaries,

Sales or Refund Vouchers, the transaction may be charged back to you. It is also essential to Cardnet, in the event that any summaries or vouchers are lost en route.

Sending your over the counter vouchers and Card Not Present Transaction Schedules to Cardnet for processing

All vouchers and Card Not Present Transaction Schedules must be posted to Lloyds Bank Cardnet, PO Box 22, Sheffield S98 1BG at the end of each business day.

Important

Do not send paper vouchers into Cardnet if a transaction has already been processed through an electronic terminal. If in doubt, please telephone the Cardnet Helpline on **01268 567100.**

Record keeping

In order to help us to defend potential chargebacks, see Section 7, 'Security, Chargebacks' (p81), on your behalf, you must keep copies of all transactions for a minimum of 13 months after the completion of each transaction.

A transaction is only completed on the final delivery of goods or services.

- In certain circumstances we will ask you to provide us with Sales and Refund Vouchers within a limited time scale. This is because strict time limits for the supply of this information are enforced by each of the Card Schemes.
- When we ask you for a copy of a Sales Voucher, the card issuer may only supply us with the transaction date and cardholder number. It is important that you store your sales slips carefully and in date order, so as to ease the retrieval process.
- If, for any reason, you are unable to provide copies of the requested information you may receive a chargeback for the transaction in question. See Section 7, 'Security, Chargebacks'.
- Under no circumstances must you retain Card Security Codes (CSC) when accepting 'Card Not Present' (CNP) transactions. Card Security Codes must be destroyed once the transaction is authorised. See Section 4, 'Accepting transactions' (p45).
- All electronic card data (such as information stored in the magnetic stripe) must be retained in a fully secure environment at all times.

For detailed information on how to store cardholder receipts and electronic card data, please see Section 7, 'Security, Storage of cardholder information' (p66).

Your Cardnet statement

Each month we will send you a Cardnet Merchant Statement. The statement breaks down your card transaction information in ways that are designed to be of most value to you. Our aim is to give you as much detail as we can so that you are in complete control of your card transactions and business analysis.

We also provide you with a separate statement guide to help you understand and get the best out of the information provided.

Please check all the details shown in the statement against your own records. If you have any queries about your Cardnet statement please contact the Cardnet Helpline on **01268 567 100,** or write, quoting your Cardnet merchant number and statement month, to:

Cardnet Merchant Services
Janus House
Endeavour Drive
Basildon
Essex SS14 3WF

Online statements

You can also access your Cardnet statement through our online reporting tool. For further details please contact the Cardnet Helpline on **01268 567 100.**

Online reporting tool

Our online reporting tool is a secure website, which will enable you to manage your card payments through Cardnet, online, 24 hours a day, seven days a week. As well as giving you access to your monthly statement, it also has the following benefits to enable you to manage your business on a day-to-day basis more effectively:

- Ability to view six months of transaction data.
- Detailed transaction information for credit, debit, chargebacks and adjustments.
- A snapshot of your processing information including recent transactions, adjustments and bank deposits.
- Scheduled reporting which can be set up to be received by email daily, weekly, monthly, quarterly or annually.
- The ability to review reports in Excel, CSV, Word and PDF formats.

Managing your Cardnet merchant account online will provide the opportunity to eventually eliminate paper statements and other costly processes. This will also mean a reduction in paper usage and a contribution to reducing your business carbon footprint.

If you would like to take advantage of our online reporting tool simply call the Cardnet Helpline on **01268 567 100.**

Manage your card payments through Cardnet, online, 24 hours a day, seven days a week

7 : Security

This section explains the security procedures you need to follow.

Data security

The card payment industry is concerned about the increasing incidents related to stolen card and cardholder information. These thefts have resulted in merchants and financial institutions suffering fraud losses and unanticipated operational expenses, and, of course, significant inconvenience to cardholders.

Storage of cardholder information

The following information must not be stored after receiving authorisation for a transaction under any circumstances:

- Information stored in the magnetic stripe that facilitates card processing.
- The Card Security Code (CSC) or CVC2 (the three-digit number indent-printed on the signature strip and used for mail/telephone orders or E-commerce transactions).

Only the information that is essential to your business, for example name, account number or expiry date, can be stored. This must be kept in a secure area limited to authorised personnel and the data masked or encrypted.

Destruction of cardholder information

You must destroy (through incineration, cross shredding or crushing) any media containing obsolete transaction data with cardholder information. This includes paper transaction records, which should never be thrown intact into the public rubbish system.

Reporting a security incident

- In the event that card transaction data is accessed or retrieved by any unauthorised entity, you must notify us immediately.
- You must also follow your business continuity plan.

This will not only minimise risk to the card payment system, but more importantly protect your customer. Systems and procedures are in place to stop the unauthorised use of compromised data, but are effective only when you do your part to promptly report a security incident.

Point of sale terminal security

Please be aware that criminals have been targeting point of sale equipment in order to commit counterfeit fraud overseas. It is important that you and your staff remain vigilant at all times and ensure that no one has the opportunity to tamper with your point of sale terminal.

If you have cause to be suspicious about an approach from an unauthorised person, please contact the Cardnet Helpline on **01268 567 100** and your terminal vendor/supplier.

Your terminal vendor will always contact you first before sending an engineer to you.

We continue to work on your behalf to reduce card fraud. This information is designed to give you a better understanding and awareness of these issues, which will help minimise risk and protect your customers.

Payment Card Industry – Data Security Standards (PCI DSS)

To protect your business, your customers (cardholders) and the integrity of the payments system, the Card Schemes (Visa and MasterCard) have introduced a set of requirements governing the safekeeping of account information, these are known as the Payment Card Industry Data Security Standard (PCI DSS).

Compliance with PCI DSS is mandatory and applies to all entities that store, process or transmit cardholder data.

We need to let you know that if your business does not comply with these standards you could receive substantial fines from the Card Schemes (Visa and MasterCard) and further fines on top of this if a compromise of cardholder data occurs. These are based on the cost of issuing replacement cards and related fraud losses.

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the PCI DSS are organised.

Build and Maintain a Secure Network	**Requirement 1:** Install and maintain a firewall configuration to protect cardholder data. **Requirement 2:** Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	**Requirement 3:** Protect stored cardholder data. **Requirement 4:** Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Programme	**Requirement 5:** Use and regularly update anti-virus software. **Requirement 6:** Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	**Requirement 7:** Restrict access to cardholder data by business need-to-know. **Requirement 8:** Assign a unique ID to each person with computer access. **Requirement 9:** Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	**Requirement 10:** Track and monitor all access to network resources and cardholder data. **Requirement 11:** Regularly test security systems and processes.
Maintain an Information Security Policy	**Requirement 12:** Maintain a policy that addresses information security.

Remember

When you engage Agents or Third Parties (software houses, payment service providers, web hosting companies, EPOS & till vendors):

- You must tell us about any Agent or Third Party that engages in, or proposes to engage in the processing or storage of card transaction data on your behalf.
- You must ensure that your Agents/Third Parties are compliant with PCI DSS and have registered with Visa as a Merchant Agent at www.visamerchantagents.com

Important next steps to ensure your business is compliant

All Cardnet merchants are mandated to validate their compliance with PCI DSS.

For most merchants this is through the completion and attestation of an annual self assessment questionnaire (SAQ) on our PCI DSS Compliance Management Service available at **lloydsbankcardnetpcidss.com**

Our online portal **lloydsbankcardnetpcidss.com**, delivered in association with our partner Sysnet Global Solutions, will give you all the information you need to become, and remain, compliant through a simple, straightforward programme. The online portal helps you to understand which requirements are appropriate to your business and guides you through your self-assessment step by step, providing support and help at every stage. It's an ongoing service which ensures that you maintain your compliance.

Compliance with PCI DSS must be maintained at all times and validated on an annual basis. This is because you may change your infrastructure and card acceptance equipment due to sales growth or card acceptance method.

Also, the Standard itself operates on a life cycle and changes from time to time to adapt to new security threats or market requirements.

Normally, PCI DSS compliance will be far easier in subsequent years and the time it takes for you to complete your compliance steps should reduce significantly.

Depending on how you accept card payments, you may also need to undertake a quarterly vulnerability scan. This is to support merchants who have a point of sale device with an Internet connection, are taking Card Not Present cardholder payments through a virtual terminal or hosting their own E-commerce payment pages.

A vulnerability scan is designed to be non-intrusive and ensures that your systems are protected from the threat of external threats (such as hacking or malicious viruses). Unlimited scanning of one IP address – nominated by you – is included in our PCI DSS Compliance Management Service.

You can find out more information about our PCI DSS Compliance Management Service in our Frequently Asked Questions section:
lloydsbankcardnetpcidss.com/services/content/faq

Please note, if your business is taking more than one million Visa, MasterCard, Discover Financial Services or partner card transactions annually (regardless of acceptance type – for example, card present, face to face, mail/telephone order) then you will need to validate your compliance with PCI DSS by having an annual onsite audit. The annual audit needs to be completed by a member of your internal staff who has achieved the recognised PCI Security Standards Council internal assessor qualification or by an approved Qualified Security Assessor (QSA).

To find a Qualified Security Assessor (QSA) please go to **www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf**

Further details and more information about the Standard itself can be downloaded via the dedicated PCI Security Standards Council website: **www.pcisecuritystandards.org**

CARDNET HELPLINE

Call 01268 567 100
8am to 9pm Monday – Saturday
Call our knowledgeable UK-based team with any questions about Data Security.

Protecting your point of sale and card processing equipment

To help all card-accepting businesses better protect themselves and their customers this guide has been developed to help minimise the chances of being targeted.

Transactions with your chip and PIN terminal

Chip and PIN has been highly successful in reducing certain types of fraud but criminals will always try to target shops and businesses in order to obtain card details and PINs to commit fraud.

These guidelines complement card industry rules and regulations and advice provided by Visa and MasterCard, Discover Financial Services and point of sale equipment providers.

Why do criminals target cards, card details and PINs?

Fraudsters try to capture card details and PINs in order to produce fake magnetic stripe cards, which can then potentially be used in shops or cash machines that haven't upgraded to chip and PIN – mainly overseas.

Threats

Listed below are some of the main forms of attack in the shop environment:

Electronic attacks

These are attacks on the chip and PIN terminal or the software used to process card details. Criminals attempt to place illegal, data-capturing devices, bugging equipment or software in chip and PIN terminals or install pinhole cameras, focused on a keypad, that record cardholders' PINs.

Substitution attack

Fraudsters attempt to remove parts or all of the chip and PIN terminal and substitute them with doctored or bogus devices that capture card data or PINs. Criminals may attempt to install fake equipment by posing as service engineers.

Theft

Criminals may try to steal chip and PIN terminals with the aim of gaining access to any stored data held in the device; learning about their inherent security features, or attempting to doctor the device prior to reinstalling it in a shop environment.

Members of staff

Criminals may target businesses by applying for jobs or coercing existing shop staff into helping them so they can access chip and PIN terminals, install pinhole cameras or skim cards through the use of handheld card readers.

Keeping chip and PIN equipment safe and secure

Chip and PIN terminals need to meet specific levels of security that are set by Visa, MasterCard, Discover Financial Services and the UK Cards Association.

On top of this it is essential that the location where they are being used is physically secure and that the devices are safely looked after. The following guidelines can help keep chip and PIN equipment safe and secure.

Physical security of equipment

- The physical location of the chip and PIN terminal and security of its parts should be considered. Can it be removed easily? Are the separate parts physically protected to prevent tampering or theft?*
- Chip and PIN terminals should always be placed in a location that allows the cardholder to use them in a way that prevents other cardholders from seeing the PIN. Where practical, terminals should include PIN shielding.
- Secure cradles should be used to minimise opportunities for criminals stealing the terminal.*
- CCTV should be used to cover the till area. Cameras must be fixed so that a cardholder's PIN cannot be identified. Access to CCTV footage should be restricted to authorised staff and measures in place to ensure that it is not possible to interfere with the recordings.†
- Routines should be implemented to check the condition of chip and PIN equipment on a regular basis to ensure that it has not been tampered with. Checks should include an inspection of the cabling to ensure that nothing has been added.
- Only authorised personnel should be allowed access to chip and PIN equipment so always ask for identification and be very suspicious of any engineers turning up without prior arrangement.
- A process that oversees any changes to chip and PIN equipment – with appropriate audit trails – should be in place, especially where external suppliers provide maintenance checks.
- Employee application processes should include checking an applicant's work history and work record, as far as allowed by law.
- A documented security policy should be developed that is available to all staff and, where possible, responsibility for security matters should be allocated to a manager who can act as a single point of contact for all staff.
- Security training should be carried out to remind staff of their responsibilities at least annually (and more regularly where staff turnover is high). This training should be an integral part of the induction of new staff.

* Care must be taken to balance these security needs with the requirements of the Equalities Act 2010.

† See also the Information Commissioner's CCTV Code of Practice **www.ico.gov.uk**

- Staff should be made aware of all the potential ways that criminals target card data and encouraged to report any issues or concerns they may have.
- Any security-related activities involving chip and PIN equipment should be carried out under the supervision of more than one employee or manager.
- Staff access to sensitive data should be managed accordingly. This includes staff who have no operational responsibility but have physical access to buildings (for example, staff not directly employed by your organisation – such as cleaning and maintenance staff).
- Staff who are approached or coerced by criminals into acting fraudulently should contact the police immediately.
- When employees leave the employment of an organisation it is important to ensure that all of their access rights and security related entitlements are revoked. In particular ensure that all keys are returned and that any physical access codes are changed so that they cannot subsequently enter secured areas.

Managing chip and PIN equipment

Chip and PIN terminals are valuable assets and should be treated as you would the cash in a till. They should also be subject to good management routines.

- Merchants should devise an inventory to record the serial numbers of their terminals and the location where they are installed (including replacements and spares).
- Regular checks should be carried out to ensure that these devices are where they should be and that any changes are authorised and noted in an asset management record.
- Shop managers should also have systems in place to review inventories and asset management records on a regular basis and have procedures in place when any inaccuracies are spotted.
- Where equipment consists of several different components, each part should authenticate itself to the terminal – this may take the form of a regular heartbeat check. Any unusual events (such as missing heartbeats) should be flagged for supervisor attention.

Staff security

A standardised recruitment and vetting procedure, including criminal record checks, should be adopted that covers all employees (full time, part time, temporary and contract).

Suspicious transactions

If you suspect something is wrong, or the card checks you make show inconsistencies, then you must telephone the Authorisation Centre on 01268 822 822 and state that "This is a Code 10 authorisation" then follow their instructions.

Code 10 authorisation must be sought in the following circumstances:

- The four digits on the signature strip on the back of the card are different from the last four digits of the card number on the front of the card.
- The cardholder's signature differs from that on the card.
- The title on the card does not match the cardholder's.
- The signed name is not the same as that embossed on the front of the card.
- The word void is visible on the signature strip or there is any indication that the strip has been tampered with.
- There has been any attempt to disguise or amend the signature.
- The card is unsigned.
- The hologram is damaged or missing.
- There is no UV mark on the card, see Section 3, 'Checking the card' (p33).
- The card has been mutilated in any way.
- You have any reason to be suspicious about the sale, the card or the cardholder.
- The amount of the transaction is significantly higher than normal for your business.
- Your terminal requests that you call the Authorisation Centre.

You must hold on to the card (and goods) and telephone the Authorisation Centre immediately on **01268 822 822** – you should not call the police unless instructed to do so by the Authorisation Centre.

When you make a Code 10 authorisation you should have the following details ready:

- The card number.
- The card issue number (if applicable).
- Your Cardnet merchant number.
- The exact amount of the transaction, in pounds and pence.
- The card expiry date.

You must tell the operator:

"This is a Code 10 authorisation."

This will alert the Authorisation Centre and you will be asked a series of questions, most of which will require 'Yes' or 'No' answers (to avoid difficulty or embarrassment if the cardholder is waiting close by).

The operator may instruct you to call the police or let you know that the police have been notified. Police involvement is not always necessary – please do not contact the police unless instructed to do so.

Reward

There is normally a £50 reward to any Cardnet merchant for cards recovered at the request of the Authorisation Centre.

Please note that Discover Financial Services do not participate in the reward scheme. This means we are unable to pay a reward for the recovery of Diners Club International, Discover, BCcard or DinaCard cards.

Recovering a stolen card

After recovering a card you should:

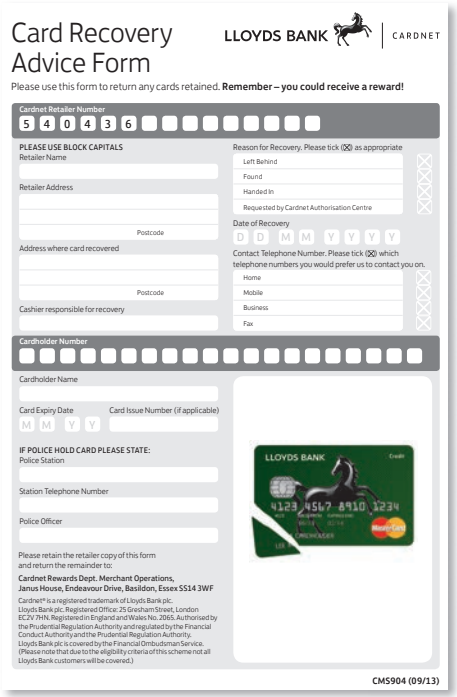
- Cut the bottom left-hand corner from the front of the card.
- Attach both parts of the card to a Cardnet Card Recovery Advice Form. You'll find two copies of the Card Recovery Advice Form in your Cardnet Starter Pack. For further copies, contact the Cardnet Helpline on **01268 567 100**.
- Return it to:

Cardnet Rewards Department

Merchant Operations
Janus House
Endeavour Drive
Basildon
Essex SS14 3WF

If the police ask for the card recovered by you, you must:

- Allow the police officer to take it.
- Obtain the officer's name and police station.
- Obtain a receipt if possible.
- Inform Cardnet at the address above left.



Card Recovery Advice Form

LLOYDS BANK | CARDNET

Please use this form to return any cards retained. **Remember – you could receive a reward!**

Cardnet Retailer Number 5 4 0 4 3 6

PLEASE USE BLOCK CAPITALS
Retailer Name
Retailer Address
Postcode
Address where card recovered
Postcode
Cashier responsible for recovery

Reason for Recovery. Please tick (⊠) as appropriate
Left Behind
Found
Handed In
Requested by Cardnet Authorisation Centre

Date of Recovery D D M M Y Y Y Y

Contact Telephone Number. Please tick (⊠) which telephone numbers you would prefer us to contact you on.
Home
Mobile
Business
Fax

Cardholder Number

Cardholder Name
Card Expiry Date M M Y Y
Card Issue Number (if applicable)

IF POLICE HOLD CARD PLEASE STATE:
Police Station
Station Telephone Number
Police Officer

Please retain the retailer copy of this form and return the remainder to:
Cardnet Rewards Dept. Merchant Operations, Janus House, Endeavour Drive, Basildon, Essex SS14 3WF

Cardnet® is a registered trademark of Lloyds Bank plc.
Lloyds Bank plc. Registered Office: 25 Gresham Street, London EC2V 7HN. Registered in England and Wales No. 2065. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.
Lloyds Bank plc is covered by the Financial Ombudsman Service.
(Please note that due to the eligibility criteria of this scheme not all Lloyds Bank customers will be covered.)

CMS904 (09/13)

A Code 10 authorisation should only be made if you are suspicious or if you have received instructions from Cardnet. You must not use a Code 10 authorisation to validate cardholder addresses or for Card Not Present transactions.

How to guard against fraud

Over the counter transactions

Please make sure that all staff accepting payment by card on your behalf have read and understood the following guidelines which aim to reduce the possibility of fraud.

These suggestions could help you to prevent fraudulent transactions that could result in a chargeback to you.

- Be extra vigilant if you are presented with a card that does not carry a chip as these are less secure and more likely to be used to perpetrate fraud.
- Ask yourself does the cardholder appear nervous/agitated/hurried?
- Is the cardholder making indiscriminate purchases?
- The cardholder makes an order substantially greater than your usual sale, for example, your average transaction is £40, but this transaction is for £400.
- The cardholder insists upon taking the goods immediately, for example, they are not interested in free delivery, alteration or if the goods are difficult to carry.
- If a voucher is being used the cardholder takes an unusual amount of time to sign and refers to the signature on the back of the card.
- The cardholder takes the card from a pocket instead of a wallet.
- The cardholder repeatedly returns to make additional orders in a short period of time causing an unusual/sudden increase in the number and average sales transactions value over a one-to three-day period.
- Never transfer funds on a customer's behalf. Such transactions (for example, on behalf of translators or couriers) are highly likely to be fraudulent.
- The sale is at an unusual time of day for your business.
- Do not under any circumstances refund a payment in part or in full to a card (or account) other than to the card used to process the original sale.
- The cardholder tells you that he/she has been having problems with his/her card for payment where multiple transactions are subsequently declined but eventually an authorisation is obtained for a lower amount. (Most genuine cardholders know how much available credit they have).
- A fraudster may present more than one card, often to find a card that will be successfully authorised. If this happens, take particular care and also look out for cards presented, issued by the same bank, where the card numbers are sequential or very similar. When in doubt, make a Code 10 call to the Authorisation Centre.
- Most floor limits are zero. However, if you have an electronic terminal with a floor limit and you wish to reduce exposure to fraud, you may request a reduction to your terminal floor limit. Not only will this reduce fraud but it may also reduce chargebacks due to invalid cards. Please contact your terminal supplier to arrange this reduction.

- You should be on guard when chip and PIN cards are presented and the PIN is blocked or the incorrect PIN is entered. You should check that this is the genuine cardholder because you are at risk if you accept a signature in these circumstances.

Remember: If the appearance of the card being presented or the behaviour of the person presenting the card raises suspicion, you must call the Authorisation Centre on **01268 822 822** and state "This is a Code 10 call" and follow the operator's instructions.

AUTHORISATION CENTRE

Call 01268 822 822
State "This is a Code 10 call" and follow the operator's instructions.

Counterfeit cards

Chip and PIN cards have reduced this type of fraud as most cases of counterfeit fraud involve 'skimming' or 'cloning'. This is where the genuine data in the magnetic stripe on one card is electronically copied onto another card without the legitimate cardholder's knowledge. This type of fraud can be identified by checking that the card number printed on the voucher is the same as that embossed on the front of the card. If these numbers differ, call the Authorisation Centre immediately on **01268 822 822** stating "This is a Code 10 authorisation".

To help avoid receiving chargebacks as a result of counterfeit fraud and disputed key entered transactions, follow the 'Failed Card Swipe Procedure', see Section 9, 'Exceptions'.

Card Not Present (CNP) fraud

Card Not Present fraud occurs when fraudulently obtained card details are used to order goods by telephone, mail order or electronically such as over the Internet.

If the goods that you sell can be easily resold such as computers, TV and hi-fi equipment, you may be especially vulnerable to being targeted by fraudsters using fraudulent or stolen cards. You should be particularly suspicious of unusually high value or bulk purchase transactions from new customers.

The Card Security Code (CSC) and Address Verification Service (AVS) will help you decide whether to progress with a transaction. See Section 4, 'Accepting transactions, Card Not Present transactions' (p43). Please do not use the Code 10 authorisation facility to undertake address checks.

Important

Under no circumstances can goods purchased by mail or telephone be handed over the counter to, or collected by, the cardholder.

If a cardholder wishes to collect the goods, then they must attend your premises in person and produce their card. Any Sales Voucher already prepared must be destroyed and an over the counter transaction processed. If you have already completed a CNP order you must either cancel the transaction or perform a refund. If you perform a refund, please let the cardholder know that the original transaction, a refund and the over the counter transaction will all appear on their card statement.

There are a number of extra checks you can make to help make sure you are dealing with a genuine cardholder including:

- Use Verified by Visa, MasterCard SecureCode and Diners Club International ProtectBuy for E-commerce transactions. See Section 4, 'Accepting transactions'.
- For business cardholders not known to you, check their details in your local business directory or Internet search engine.
- Private cardholders' addresses not known to you can be checked against the Electoral Register, telephone directory, from a BT CD-ROM phone disk or Internet map searches.
- Obtain a telephone number for the cardholder's address using a Directory Enquiry Service, if possible, and telephone the cardholder back on that number to confirm the order (not necessarily straightaway).
- Be aware if the cardholder is suggesting unusual arrangements such as going back for another card number if the one given is refused.
- Check your records to see if you have had a number of transactions over a short period of time from a company or individual with whom you have not had any previous dealings.
- Also check to see if there are any unusual features or consecutive sequences in the card numbers given over a period. (Usually fraudsters will offer card numbers that are the same except for the last four digits. This could mean that a batch of cards has been stolen).
- Be especially wary if the delivery or cardholder's address given is overseas and products purchased are readily available in that locality.

Also be particularly wary of:

- Demands for next day delivery.
- Alterations of delivery address at short notice.
- Phone calls on the day of delivery asking what time the goods are due to be delivered.
- Multi-tiered address for example, units, flats.

Danger signals

If any of the following happen, we recommend you make extra checks. This list does not cover every eventuality – some fraudsters spend a long time building up credibility and then request an extremely large order that is 'too good to be true'.

- Is the sale almost too easy? Is the caller disinterested in the prices/precise details of the goods, particularly if it is a new customer? Is the stock ordered of high value or easily resold merchandise?
- Is the sale excessive in comparison with your usual orders? Is the cardholder ordering lots of different items? Does the spending pattern fit your average customer?
- Is the customer giving you a third party's card number, claiming to be acting on behalf of a 'client'?
- Does the caller match the card? Do not accept orders from someone quoting someone else's card details, for example, a woman using her husband's card or a business using a personal card. It may well be a genuine call, but it pays to check.

- Never split an order to avoid authorisation, or at the suggestion of the cardholder – for instance, if they offer two card numbers to cover one order.
- Is the caller suggesting any unusual arrangements? For example, "if the card number I've given you doesn't have sufficient funds let me know and I'll give you another number".
- Is the caller being prompted by a third party whilst on the telephone?
- Does the caller seem to have a problem remembering their home address or telephone number or do they sound as if they are referring to their notes?
- Does the cardholder seem to lack knowledge of their account?
- Is the card-issuing bank/building society based overseas?

Please remember you remain ultimately responsible should a transaction be confirmed as invalid or fraudulent, even if the AVS and CSC data matches and an authorisation code is given.

Delivery warning signals

Here are some danger signs to look out for when arranging delivery of goods.

- Goods should not be released to third parties such as 'friends' of the cardholder, taxi drivers, chauffeurs, couriers or messengers. (However, third party delivery of relatively low value goods such as flowers is appropriate).
- Insist that goods may only be delivered to the cardholder's permanent address. If you agree to send goods to a different address, take extra care and always keep a written record of the delivery address with your copy of the transaction details.
- Don't send goods to hotels or other temporary accommodation. Only send goods by registered post or a reputable courier and insist on a signed and dated delivery note.
- Be wary of sending goods abroad that may be readily available in the buyer's local market.

Couriers should be instructed:

- To make sure the goods are delivered to the specified address and not given to someone who 'just happens to be waiting outside'.
- To return with the goods if they are unable to effect delivery to the agreed person/address.
- Not to deliver to an address which is obviously vacant.
- To obtain signed proof of delivery, preferably the cardholder's signature.

Other important fraud considerations

Remember – an authorisation code only indicates the availability of a cardholder's credit and that the card has not been blocked at the time of the transaction. It does not guarantee that the person using the card is the rightful cardholder.

Do not, under any circumstances, process transactions for any business other than your own. Some fraudsters offer commission to process transactions while they are awaiting their own credit card facilities or where they have not been successful in obtaining their own. If you process transactions on behalf of any other business/person you will be liable for any chargebacks and could put your own Cardnet facility at risk.

Fraud prevention

Transaction laundering

If you are approached with a proposal to buy card transactions, you must contact us immediately on **01268 567 100.** This is a form of money laundering and is contrary to the terms of your Retailer Agreement.

Phishing emails

If you receive an email from somebody claiming to be a bank or an official business asking for transaction details of all cards recently accepted for payment, you must report this to Cardnet straight away on **01268 567 100.** This is a fraud tactic to obtain card details. A bank or any other official business would never make contact in this way to request card information.

Fraud prevention programmes

Some businesses are more prone to fraud than others and you may be unfortunate enough to suffer a fraud attack, particularly if you offer goods that are attractive to fraudsters and can be easily, but illegally, resold.

It is your responsibility to protect your business from financial loss. It is also imperative that you and any staff that you employ follow the contents of this manual carefully at all times.

If you are concerned that you may be vulnerable to fraud attack, perhaps because of your business location or local intelligence, please contact the Cardnet Helpline and ask to speak to our Fraud Department who will be happy to help with guidance on best practice.

Please remember – following the procedures contained in this manual is no guarantee that you will avoid incurring financial loss if you suffer a fraudulent transaction. You will remain ultimately responsible for any financial loss you incur as a result of any fraudulent transaction.

Further information on fraud prevention can also be found at **www.financialfraudaction.org.uk** as well as in literature for staff awareness.

Chargebacks

A cardholder, or the card-issuing bank has the right to question/dispute a transaction. Requests for a copy of the transaction can be received up to 180 days after the transaction has been debited to the cardholder's account and in some circumstances beyond 180 days.

The following section describes the procedures which you must follow together with suggestions which will help you reduce the risk of chargebacks being debited from your account.

Remember, you may be liable for a chargeback in some circumstances even if you obtained authorisation for a transaction, and followed all of the processes and procedures in this manual and your agreement with us.

Retrievals

In many cases, before a chargeback is initiated, the card-issuing bank requests a copy of the sales slip, via a 'retrieval request'. Once a retrieval request is received from the card issuer, we will respond by sending a copy of the transaction, if available.

Where you hold terminal receipts for electronically processed transactions or E-commerce authentication data, it is your responsibility to respond to all retrieval requests received from Cardnet within 14 calendar days of our initial request. You are responsible for retaining and providing copies of transactions for a minimum of 13 months from the original transaction date.

Please fax copies of requested documentation to the fax number provided on the Cardnet retrieval request letter or, alternatively, you may mail your response to Cardnet:

Cardnet Merchant Services, Janus House, Endeavour Drive, Basildon, Essex SS14 3WF.

We recommend recorded delivery or registered post when you send us evidence of high value transactions.

If you fax your response, please set your fax machine to print your fax number and name on the documents you send. We can use this information to contact you in the event the transmission is not clear or complete. Also, when using the fax machine, please set the scan resolution on the machine to the highest setting. The higher resolution setting improves the clarity of characters and graphics on the sales documents transmitted and helps reduce chargebacks for illegible copies.

If Cardnet does not receive a clear legible copy of the sales slip within 14 calendar days of the initial retrieval request you may be subject to a chargeback. A courtesy call or letter may be sent if the retrieval request is not responded to within that time. However, the potential liability remains with you if the item is not supplied in time and you may become liable for the chargeback simply by failing to meet the payment scheme time frame.

Chargebacks for 'non-receipt of requested item' cannot be reversed unless the requested documentation is provided within 14 calendar days of the initial request.

Please remember: Due to time frames imposed by MasterCard, Visa and Discover Financial Services it is extremely important that you respond to/resolve a retrieval request or chargeback enquiry immediately. The more information we have at the time of the retrieval request or chargeback, the better we can dispute the item on your behalf.

We recommend that when you send a copy of a transaction, you send all the relevant documents (for example, till receipt together with any supporting invoices/sales tickets) as evidence of the transaction including any documents signed by the cardholder. In the case of Card Not Present (CNP) transactions, details of the goods ordered together with evidence of delivery, for example, a signed delivery receipt, should also be sent.

Chargeback/reversal procedure

When we receive a chargeback from a card issuer we will normally debit your bank account and let you know accordingly. Our letter will provide details of the transaction in dispute, together with the information/documentation required from you. Our letter will also tell you the latest date by which you must reply with the information/documentation needed.

If the information provided is:

a. sufficient to warrant a reversal of the chargeback and

b. within the applicable time frame

we will defend (reverse) the chargeback, if possible, but reversal is dependent upon the card-issuing bank's agreement. A reversal is not a guarantee that a chargeback has been resolved in your favour. If the chargeback is reversed, the card-issuing bank has the right to present the chargeback a second time and your account will be debited again if you have not complied fully with the terms of your Cardnet Retailer Agreement and this Operating Manual.

Please refer to the situations described in the table detailed on pages p83 to p84 which highlight the common reasons for chargeback disputes and how they can be avoided. In the majority of cases, where the cardholder is present, you can reduce your exposure to chargebacks by following the guidelines in the table.

We will do our best to help you to defend a chargeback. However, due to the short time frames and the supporting documentation necessary to successfully (and permanently) reverse a chargeback in your favour, we strongly recommend you take the following steps to reduce your chargeback risk:

- Convert or upgrade your over the counter terminal to accept chip and PIN transactions electronically.
- Ensure transactions are completed in accordance with the terms of your Retailer Agreement/Operating Manual.
- If you do receive a chargeback, always investigate and send in the appropriate documentation within the required time frame.
- Whenever possible, contact the cardholder directly to resolve the inquiry/dispute but still comply with our request for information just in case this does not fully resolve the matter.
- If you take payments from credit and debit card holders over the Internet we recommend that you introduce Verified by Visa, MasterCard SecureCode and Diners Club International ProtectBuy for your transactions. MasterCard SecureCode is mandatory for accepting Maestro and International Maestro.

Common causes and reasons for chargebacks

Reason	How to reduce your chargeback risk
The card account number indicates that it has chip and PIN capability but is subsequently found to be fraudulent.	▪ Upgrade your over the counter terminal to chip and PIN capability
Refund not processed – the cardholder is claiming that a Refund Voucher or refund acknowledgement issued by you was not processed.	▪ Ensure proper disclosure of your refund policy is on the transaction receipt, for example the words 'NO EXCHANGE, NO REFUND' must be clearly printed on the Sales Voucher or terminal receipt ▪ Process refunds immediately ▪ Refunds must be applied to the same cardholder account as the original sale ▪ Do not issue in-store or merchandise credit ▪ Do not issue a cash or cheque refund, if the original transaction was made by card
Transaction not authorised.	▪ Authorise all transactions which are equal to or above your floor limit and use the proper method of authorisation ▪ Clearly write the authorisation number on your paper vouchers
Non-receipt of goods – cardholder is claiming they did not receive the goods or goods were paid for by other means.	▪ Do not process a transaction until the goods are dispatched ▪ Do not process any card transaction where the cardholder has already paid for the goods or services using another method of payment ▪ Obtain the cardholder's signature on your delivery note
Card used before effective date or after expiry date.	▪ Carefully examine the card for the effective start and expiry dates when accepting it for a transaction ▪ Do not process a transaction prior to the effective date appearing on the card ▪ Do not process a transaction after the expiry date appearing on the card
The merchant fails to respond to requests for a copy of the sales slip.	▪ Prepare clean, legible sales slips at the point of sale and store in a secure and orderly fashion so that you are able to respond to retrieval requests within the required time frame ▪ To identify a transaction you will be given the cardholder number, date and amount of the transaction. (Card issuers are not obliged to supply cardholder names or addresses so it is important that you store your records carefully)

Common causes and reasons for chargebacks (continued)

Reason	How to reduce your chargeback risk
Cardholder did not authorise the transaction (primarily CNP transactions).	▪ Mail/telephone orders – follow the recommended procedures in Section 4, 'Accepting transactions', Card Not Present (CNP) transactions ▪ E-commerce transaction – implement Verified by Visa, MasterCard SecureCode and Diners International ProtectBuy to authenticate payments. See Section 4, 'Accepting transactions', pages p51 and p52
Non-matching account number – this is where a transaction has been processed on a non-existent card account. By way of example, it is possible that a card has been created by a fraudster or that an existing cardholder's account details have been 'skimmed', i.e. copied on to another card.	▪ If you use an electronic terminal, the chip card must be inserted into the chip reader or, if you do not have a chip terminal, swipe the card through the swipe slot and ensure the displayed card number matches the number on the card ▪ Alternatively, you can compare the card number with the number on the sales slip produced by the terminal ▪ If the chip or magnetic stripe cannot be read, for example, failed read or the terminal is inoperable, follow procedures in Section 9, 'Exceptions' ▪ Carefully examine the front and back of the card at the time of the transaction. Follow the procedures in Section 3, 'Checking the card' ▪ Check the signature ▪ Telephone orders – confirm the account number provided by the cardholder by repeating the number back to them ▪ Properly authorise all transactions
Transaction was processed more than once to the same cardholder.	▪ Settle and reconcile batches of sales and refunds on your terminal/register daily. Ensure that the total amount submitted (displayed on terminal) balances with/matches to the card receipts. See your terminal operating instructions
Sales slip was not imprinted. The sales slip provided was not imprinted using a manual imprinter machine nor was the card or magnetic stripe read (for example, the transaction was key entered into your terminal and the cardholder denies participation in the transaction).	▪ If you are unable to read a card through your terminal or capture the cardholder's information via the magnetic stripe, you must imprint a Cardnet Sales Voucher with the cardholder's card to prove the cardholder was present at the time of the transaction ▪ Manually key entering the information into the terminal does not protect you from this type of chargeback. See Section 9, 'Exceptions' ▪ If you need an imprinter these can be purchased by calling the Cardnet Helpline on **01268 567100**

A transaction will also be regarded as invalid and may be charged back to you if:

- The signature is incompatible with the signature on the card.
- The Sales Voucher sent to Cardnet differs from the cardholder's copy.
- The card is not yet valid, or has expired at the time of the purchase.
- You have been advised that the card is void.
- The sale is equal to or exceeds your floor limit and authorisation has not been obtained.
- The Sales Voucher is incomplete – for example, it is unsigned, has not been imprinted, is not dated, or the authorisation code obtained is not quoted on the voucher.
- The Sales Voucher is completed for an illegal transaction.
- Two or more vouchers have been made out for a purchase which exceeds the floor limit.
- You have in any way failed to comply with this Operating Manual or are otherwise in breach of your Retailer Agreement with Cardnet.
- The correct authorisation telephone number was not used.
- You are unable to provide a copy of the transaction proving that the cardholder authorised the sale.
- There was a delay in presenting the original transaction and it is then disputed by the cardholder/card issuer.
- The goods or services have not been supplied, or are defective or not as described.
- The voucher was not sent to Cardnet for processing on the day of the transaction and consequently rejected by the card issuer for late presentation to the cardholder's account.
- It is clearly evident that the transaction was made with a counterfeit card.
- For any reason you process a transaction on the same card number that has failed both chip/PIN and magnetic swipe.
- The transaction in respect of which the Sales Receipt was issued is for any reason illegal or of no legal effect.
- The cardholder denies having authorised the transaction and you are unable to provide evidence satisfactorily to the Bank that the transaction was authorised.
- The transaction is a Card Not Present sale and is disputed by the cardholder and/or card issuer.

Please note

Authorisation does not confirm the identity or authority of the cardholder and therefore is not a guarantee of payment. It confirms that the funds are available on the account and that the card has not been reported lost or stolen at that time.

Please remember, due to the time frames imposed by MasterCard, Visa, Maestro and Discover Financial Services it is extremely important that you respond to/resolve a retrieval request or chargeback enquiry immediately. The more information we have at the time of the retrieval request or chargeback, the better we can dispute the item on your behalf.

For further information about reducing your chargeback risk, contact the Cardnet Helpline on **01268 567 100**.

What customers want

With Cardnet you can offer more services like Cashback, mobile phone top-up and foreign currency transactions.

8 : Additional facilities for you and your customers

Cardnet offers more than just quick and convenient payments.

You can offer your customers more with these additional facilities, available with prior written agreement from Cardnet.

Purchase with Cashback*

Provided you have received written agreement from Cardnet you may, when presented with a Visa Debit, Debit MasterCard, Maestro or V PAY card as a means of payment, offer the Purchase with Cashback service.

Complete the transaction the same way as a standard purchase, but you must also take the following additional steps:

1 Cashback: can only be provided in conjunction with a purchase. The cash amount should be entered in accordance with your terminal operating instructions. This amount must not exceed your cash ceiling limit. (Your cash ceiling limit is the maximum amount of cash you can provide as part of a Purchase with Cashback facility.)

2 Authorisation: all Purchase with Cashback transactions must be authorised.

3 Charges: you are not permitted to charge cardholders for the Cashback service.

4 The Cashback amount and total transaction amount (retail purchase plus Cashback amount) must be shown separately on the transaction receipt.

5 Fallback procedure: the fallback procedure detailed in Section 9, 'Exceptions', applies to the Purchase with Cashback facility. However, manual authorisation must be obtained for all transactions that include Cashback.

Mobile phone top-up*

Electronic mobile phone top-ups are available on selected terminals, enabling you to top up your cardholder's mobile phone.

E-Top-Up

E-Top-Up is the electronic system that allows a mobile phone user to top up their phone through a terminal using a plastic card. The cardholder's network provider or a merchant offering the service will have supplied this card. The card is linked to their mobile phone.

Making an E-Top-Up transaction

- Cardholder pays you by cash, cheque or debit/credit card.
- Your cardholder's top-up card is swiped through the terminal.
- The amount they wish to top up should then be entered into the terminal.
- The top-up amount is automatically added to their mobile phone.

* Purchase with Cashback and mobile phone top-ups are not supported by Discover Financial Services or partner cards.

E-Voucher

E-Voucher allows prepay mobile users to top up their mobile phone, even if they don't have a swipe card.

Making an E-Voucher transaction

- Choose the network via the terminal menu and the desired top-up amount using the designated function keys. (These will be detailed in the user manual supplied with your terminal).
- An E-Voucher will then be printed out in the form of a receipt.
- The cardholder then pays you and you hand the E-Voucher to the cardholder.

The cardholder then calls the Interactive Voice Response (IVR) number as detailed on their receipt and enters their unique PIN, also printed on their receipt. This will then top up the cardholder's mobile phone.

At the end of the day you simply print out the end of day report from the terminal and this shows you the amount of E-Top-Ups and E-Vouchers you have sold.

This service could help you generate extra revenue through commission. If you are interested in this service call the Cardnet Helpline on **01268 567 100** for further information.

Recurring transactions

If you are a merchant who wants to accept recurring transactions and charge a cardholder's account periodically for recurring goods or services (for example, monthly insurance premiums, yearly subscriptions, annual membership fees, etc.), you will need a separate merchant account for these dedicated payments and Cardnet's agreement to accept this category of payments.

Recurring payments can be accepted on Visa Debit, Visa Credit, Debit MasterCard, MasterCard Credit, Maestro, Diners Club International, Discover, BC Global and DinaCard cards.

To ensure that you comply with current Card Scheme regulations and your cardholders' requests, please remember to follow these requirements at all times.

You must:

- Ensure that clear contact details are available for cardholders to amend or cancel payments and that their instructions are carried out properly. You should also ensure that the cardholder understands the ongoing nature of the commitment they have taken.
- Obtain an authorisation for every recurring transaction.

You must not:

- Include partial payments for goods or services purchased in a single transaction.
- Accept instructions for recurring transactions on V PAY cards.
- Impose a finance charge in connection with a recurring transaction.

- Complete a recurring transaction after receiving a cancellation notice from the cardholder or issuing bank. If a request for authorisation has been declined or if a previous transaction using an existing cardholder instruction has resulted in a chargeback to you, you must approach the cardholder to obtain a new authority.
- Key enter a recurring transaction into a point of sale terminal. You will need a software solution from one of our approved third party payment service providers (PSPs) to manage these payments on a recurring basis. Please contact your chosen PSP to see if they can support this service.

Best practice for recurring transaction merchants is to obtain a written authority from the cardholder for the goods or services to be charged to their account. In the case of E-commerce merchants, the authority should be contained within the website and an electronic or hard copy held.

The written authority signed by the cardholder must at least specify:

- The transaction amounts.
- The frequency of recurring charges.
- The duration of time for which the cardholder's permission is granted; however, this must not exceed one year.

If the recurring transaction is renewed, the cardholder will need to complete a new authority for the continuation of such goods or services to be charged to their account.

Recurring transactions are a convenient way to collect payments but they can be a source of cardholder disputes.

To address some of these concerns, both Visa and MasterCard have introduced solutions which enable merchants to validate and update the historic card details they have on file.

These solutions are known as Visa Account Updater (VAU) and MasterCard Automatic Billing Updater (ABU). There is no equivalent solution for Discover Financial Services or partner cards.

How do VAU and ABU work?

Transactions are submitted by merchants through our approved third party PSPs to the Card Schemes for validation and checking. Through this validation, you can clearly see when a new card number has been issued, when an account has been closed or when the cardholder has asked for a payment to be terminated. You can then update the card details you have on file and proceed with authorisation of the transaction.

VAU and ABU can help increase your recurring transaction approval rates and improve cardholder satisfaction.

Polling

In some circumstances, additional functions required from your electronic terminal may mean that you will need a polling bureau to process your transactions. Please note, use of a polling bureau is subject to Cardnet's agreement.

Authorisation will be sought on transactions equal to or above your floor limit and all transactions will be held in the terminal until such time as they are collected by the bureau.

Depending on your terminal type or business needs, you will be able to make an arrangement with the polling bureau for your transactions to be polled at certain times of the day or week.

Frequency of polling, the method and timing by which the transaction details are obtained and the method of crediting your bank account vary between polling bureaux. Specific details will be found in your agreement with your polling bureau.

In the unlikely event of a failed poll, the polling bureau should attempt to re-poll on your behalf. If the transaction data has still not been collected then they will contact you to determine the cause of the failure and advise you of any further action to be taken.

Gratuities

The transaction amount may be changed in order to add a gratuity if:

- You have been authorised by Cardnet to do so.
- Your terminal provides this function.
- The cardholder has given permission.

Dynamic Currency Conversion (DCC)

With DCC you can offer more choice and flexibility to your international customers. They can choose to pay you in their own currency using Visa, Mastercard, Discover Financial Services and partner cards.

Your customers will be shown the price in Sterling and their own currency, along with the exchange rate used, at the point of sale. Your terminal is automatically updated with exchange rates so you don't need to continually amend your pricing when rates fluctuate.

Commission is normally paid to you for every DCC transaction you process.

Call the Cardnet Helpline on **01268 567 100** to find out more about DCC for your business.

Accepting currency transactions

We can help you trade more easily with overseas customers by accepting payments in different currencies. Cardnet supports a wide range of transaction currencies and funding options, which can be tailored to suit your business.

Call the Cardnet Helpline on **01268 567 100** to find out more.

Cash Advance

The Cash Advance facility is available to Bureaux de Change merchants only. This facility allows you to accept cards to dispense travellers cheques, foreign currency, travel money cards and money orders.

There are specific requirements for these types of transactions. For example, secondary identification. If you are interested in this facility, please contact the Cardnet Helpline on **01268 567 100.**

Additional cards

You may also want to accept American Express or JCB cards at your point of sale. Before you can do this you will need to apply for acceptance facilities with each of these schemes and also confirm your terminal can support them.

For further information please go to the following websites:

American Express
www.americanexpress.com

JCB
www.jcbinternational.com

9 : Exceptions

How to proceed when your terminal is unable to read the chip or magnetic stripe.

Most of the cards presented to you that are chip read or swiped will process without any problems. However, if there are occasions when your terminal is unable to read the chip or magnetic stripe, please ensure you follow these procedures.

To help reduce losses through fraud and chargebacks, the table below shows you at a glance the action you need to take for the following card types for failed chip read and magnetic stripe transactions:

- Visa Credit.
- Visa Debit.
- MasterCard Credit.
- Debit MasterCard.
- Maestro.
- Diners Club International.
- Discover.
- BC Global Card.
- DinaCard.

	Revert to mag-strip*	Revert to PAN key entry
Chip cards unable to read	✔	✘
Magnetic stripe cards unable to read mag-stripe	N/A	✔†

The following guide shows you at-a-glance the action you need to take for the following cards:

- Internationally issued Maestro.
- Visa Electron.

	Revert to mag-strip*	Revert to PAN key entry
Chip cards unable to read	✔	✘
Magnetic stripe cards unable to read mag-stripe	N/A	✘

There is no fallback action for V PAY. If the chip cannot be read, please ask for an alternative method of payment.

*When swiping a card through the terminal, you may be prompted to key enter the last four digits of the number embossed on the front of the card. The terminal will then check these numbers against those held in the card's magnetic stripe.

† Ask the cardholder for an alternative method of payment or key enter the transaction into the terminal and take an imprint of the card for your records.

Failed chip card read

1 If the card offered contains a chip, the card must be entered into the chip card reader. If for any reason, the chip on the card cannot be read, where permitted, you may revert to the magnetic swipe method.

2 After three unsuccessful attempts to swipe the card, your terminal will indicate that it has not been possible to read the magnetic stripe on the reverse of the card. If the card is still unable to be read you must request an alternative source of payment.

Please note: if you swipe or key enter a chip card and the transaction is later found to be fraudulent, the transaction may be charged back to you.

Failed magnetic stripe transactions – key entry (excluding internationally issued Maestro and Visa Electron cards)

1 After three unsuccessful attempts to swipe the card, your terminal will indicate that it has not been possible to read the magnetic stripe on the reverse of the card.

2 Check the card by following the step-by-step instructions in Section 3, 'Checking the card' (p33). Only when you are satisfied with all checks, should you proceed to key enter the card details.

3 You must manually key enter the card details in accordance with your terminal operating instructions, ensuring they have been entered correctly.

4 Once you have key entered the transaction details, you must ask the cardholder to sign the terminal sales receipt and check that the signature matches the one on the reverse of the card.

5 When key entering the card number into a terminal it is necessary to take an imprint of the card and obtain a signature on the terminal receipt in order to be able to prove (if required) that the card and cardholder were both present at the time of the transaction. Do not take a photocopy instead of an imprint as this will not be sufficient proof that the card was present and could result in a chargeback.

6 Using a standard Sales Voucher and imprinter, take an imprint of the cardholder's card.

7 Complete the Sales Voucher with the amount of the transaction and record the terminal sales receipt number in the Quantity and Description box. Finally, write clearly across the left-hand side of the Sales Voucher, the words 'FAILED ELECTRONIC SWIPE'.

Do not ask the cardholder to sign the Sales Voucher. This is not required as the terminal sales receipt is the only item that requires a signature.

8 Explain to the cardholder why this process is taking place and reassure them that the Sales Voucher will not be banked but will be held as a record which will be produced to Cardnet if the transaction is disputed. (If, in conversation, it transpires that the cardholder is suffering recurring 'card read' problems it would be helpful to suggest they contact their card issuer). If you feel that there may be a problem with your terminal, please contact your terminal supplier helpline.

9 Give the cardholder the top copy of the Sales Voucher and also the relevant copy of the terminal sales receipt.

10 Attach the retailer copy of the terminal Sales Receipt to the retailer copies of the Sales Voucher. These copies must be retained for a period of not less than 13 months and must be produced to Cardnet upon request. If you fail to produce copies of the terminal Sales Receipt and Sales Voucher, the disputed transaction may be charged back to you.

Please note: if you key enter a magnetic stripe card, you do so at your own risk. Any transaction which is later found to be fraudulent may be charged back to you.

If you do not have an imprinter you should request an alternative method of payment. Alternatively imprinters can be purchased by calling the Cardnet helpline on **01268 567 100**.

If you need help or have any questions about the information in this section, please contact the Cardnet Helpline on **01268 567 100**.

If a key entered transaction is disputed and you have not completed this procedure, the disputed transaction may be charged back to you.

Important

- Please take extra care if the chip and/or magnetic stripe fails to 'read' because the card may have been deliberately damaged.
- The imprinted Sales Voucher is only a record of the transaction. Please do not process this voucher for payment.
- Merchants with electronic terminals should ensure that they have a sufficient supply of paper vouchers in order to continue to accept cards in the event of terminal malfunction.
- If your agreement with Cardnet allows you to process transactions through an electronic terminal, you may only process paper transactions for a failed magnetic stripe card transaction.

Using the paper fallback system to process over the counter transactions when your terminal is not working

Please note this is not permitted for internationally issued Maestro, Visa V PAY, Visa Electron, Diners Club International, Discover, BC Global and DinaCard cards.

If your terminal is not functioning correctly, or if you have a power or telephone network failure, you may have to use the paper fallback system and complete the transaction using a Sales Voucher. This process must be for Sterling (£) transactions only.

Over the counter transactions

A transaction can be completed by using the standard Cardnet Sales Voucher.

The Sales Voucher contains the following copies:

1 Cardholder's Copy (top copy): a record of the transaction to be given to the cardholder.

2 Processing Copy (white): a copy to be sent to Cardnet.

3 Retailer's Copy (yellow): a copy of the transaction for your records. A copy of the transaction must be produced to Cardnet if requested and therefore must be kept for at least 13 months. If you are unable to produce a copy the transaction may be charged back to you.

4 Retailer's Duplicate Copy (blue): a further record if you should need one.

Completing the Sales Voucher

1 Complete the Sales Voucher with a ballpoint pen as shown in the illustration, giving brief details of the goods purchased. Do not mark copies with pencil, paper clips or staples, as these can transfer through the carbons and obscure details.

2 Check that all details are clear especially on the processing copy of the voucher set. If the detail is not clear, a chargeback may occur. If you make a mistake please complete a new voucher and destroy the old one.

3 Retain the card and check the card details carefully as detailed in Section 3, 'Checking the card' (p33). Ask the cardholder to sign the voucher.

4 When the voucher is signed check that the signature is compatible with the one on the card. If the cardholder's title is shown on the card, ensure that the presenter of the card matches the title, for example, if 'Mr' is printed, ensure the presenter is male.

5 You'll need to obtain an authorisation for every paper fallback transaction you take. The telephone number to call is **01268 822 822**. (Please refer to your Retailer Agreement for your Cardnet floor limits).

6 The operator will ask you for the details needed to authorise the transaction.

Occasionally the operator may ask you to obtain further identification from the cardholder or ask to speak with the cardholder directly. If this happens, please co-operate as fully as possible and ensure that the telephone handset is passed back to you to speak with the operator to confirm the conversation with the cardholder and obtain the authorisation number from them, if given, before replacing the receiver. The operator may also ask you to check some additional forms of identification, for example, a driving licence.

7 If the operator authorises the transaction, write the code in the space provided on the voucher.

8 When you are satisfied that everything is in order, hand the cardholder the top copy of the voucher and their card.

9 Once the cardholder has left, do not alter the copies in any way. If there are subsequent queries or disputes, the cardholder's copy will normally be treated as correct.

Please note

- If you print vouchers on your own tills, then the name and address of your outlet must appear on all copies.
- If voucher details are not able to be clearly read, this may result in a chargeback to you.

Authorisation is not a guarantee of payment. It confirms that the card has not been reported lost or stolen at the time of the transaction and that adequate funds are available.

If the sale is declined

No reason will be given if the sale is declined. In these circumstances, please return the card to the cardholder, discreetly explaining that the card issuer has declined the transaction, and ask for another method of payment.

The operator may ask you to keep the card. Again this should be done as politely as possible and only if you feel you face no physical risk. After the cardholder has left, cut the bottom left hand corner from the front of the card. Attach the two pieces of the card to a completed Cardnet Card Recovery Advice Form (see page p74 for details on how to request further copies), and return it to the address on the form.

Remember a £50 reward is normally paid to any Cardnet merchant when a stolen card is recovered.

Please note: Discover Financial Services do not participate in the reward scheme. This means we are unable to pay a reward for the recovery of Diners Club International, Discover, BC Global Card or DinaCard cards.

Paper refunds

The Refund Voucher consists of four parts; a top copy printed in red for the cardholder, a white copy for processing, and yellow and blue copies for your own records.

Completing a refund

If you wish to complete a refund using the paper fallback system, you must follow the steps below.

1 Check the card following the instructions in Section 3, 'Checking the card' (p33).

2 Complete the voucher: Refund Vouchers must be completed in the same way as Sales Vouchers. Make a brief note on the Refund Voucher about the exchange and/or return of any items. Do not mark copies with pencil, paper clips or staples, as these can transfer through the carbons and obscure details.

3 Authorisation: where an authorisation code was obtained for the original transaction, telephone the Authorisation Centre on **01268 822 822**. See Section 5, 'Authorisation and referrals' (p55).

4 Signature: you must sign the Refund Voucher.

5 Return the card: once you have completed all the above steps, return the card to the cardholder together with any original receipt and a signed copy of the refund slip.

If the cost of the replacement item differs from the returned item, a refund for the original item should be completed on the same card as the original transaction. A new sale should be completed for the new transaction and authorisation obtained.

Remember: never refund a card where the original transaction was made by another method of payment. For example, cash or cheque.

Authorisation is not a guarantee of payment. It confirms that the card has not been reported lost or stolen at the time of the transaction and that adequate funds are available.

Processing Card Not Present (CNP) transactions when your terminal is not working

Provided you have received written agreement from Cardnet you may accept a telephone or written order from a cardholder who wishes to pay using a Visa, MasterCard, Maestro, Diners Club International, Discover, BC Global, or DinaCard card. Visa Electron cards can be accepted for CNP, as long as you authorise the transaction, see Section 5, 'Authorisation and referrals'.

You must not accept internationally issued Maestro or V PAY cards for CNP transactions.

To process your CNP transactions you need to record the information on form CMS910 'Card Not Present Transaction Schedule'.

These forms are available by calling the Cardnet Helpline on **01268 567 100.**

The CMS910 is a two part carbonated form containing a perforated section which allows you to record the cardholder's Card Security Code (CSC) on the top copy only. This means that the CSC will only be recorded on the copy that you send to Cardnet for processing. This ensures that you comply with the Card Scheme regulations which state that the CSC information must not be stored by a merchant (the perforated section on the top copy that you send through to Cardnet is destroyed once the transaction has been processed).

It is important that you use the CMS910 to process these transactions, as the standard Sales Vouchers do not comply with the Card Scheme regulations in relation to the non-storage of the CSC data. For all CNP orders using the CMS910 you must collect the card and cardholder details following the instructions in Section 4, 'Accepting cards, Card Not Present transactions' (p43).

1 Complete a Cardnet 'Card Not Present Transaction Schedule' CMS910.

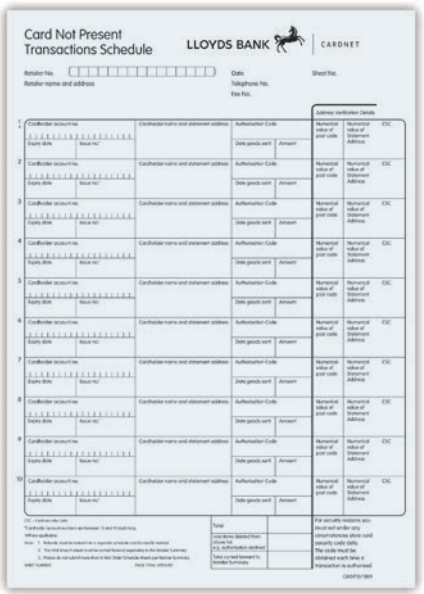
2 At the end of the day total up each sheet and list each CNP transaction separately on a Retailer Summary Voucher. (Please do not submit more than 16 schedules behind one Retailer Summary Voucher).

3 Any refunds must be entered on a separate sheet which should be clearly marked 'Refunds' and sent to us for processing with the sales pages. The value of refunds must be offset against the value of sales.

4 Keep the carbon copy of the schedule for your records. These must be kept for a period of 13 months as Cardnet may ask you to provide a copy of the transaction in the event of a dispute. For details on how this information must be stored see Section 7, 'Security'.

5 Send the top copies and Retailer Summary Voucher into Cardnet at the following address: Lloyds Bank Cardnet, PO Box 22, Sheffield S98 1BG.

6 Send a receipt to the cardholder to confirm the order. Please remember that for security reasons the cardholder receipt must not include the full card number.


Card Not Present Transactions Schedule

LLOYDS BANK | CARDNET

Authorising Card Not Present transactions when your terminal is not working

Authorisation must be obtained for all sales by calling **01268 278 278.** This enables you to carry out the usual status check so that you can confirm whether your customer has the funds to pay you. It also allows you to find out whether or not the card has been reported lost or stolen.

When you call the Authorisation Centre, the operator will ask you for the card and cardholder information needed to authorise the transaction(s).

If you use the Address Verification Service the operator will check the details you have provided, and give you one of the authorisation responses detailed in the table in Section 4, 'Accepting transactions, Card Not Present transactions' (p43).

You can then make an informed decision whether or not to accept the card as payment.

However, please remember that you remain ultimately responsible should a transaction be confirmed as invalid or fraudulent, even if the data matches and an authorisation code is given.

Important: if you choose to deliver goods to an address other than the cardholder's address, you are taking additional risk. See Section 7, 'Security, How to guard against fraud', for some helpful tips.

Banking

Please remember to submit your Retailer Summaries, Sales Vouchers, Refund Vouchers and Card Not Present Transaction Schedules to Lloyds Bank Cardnet, PO Box 22, Sheffield S98 1BG at the end of each business day.

For full details on how prepare these transactions for processing, please refer to Section 6, 'Banking and reconciliation' (p59).

10 : Additional information

Keeping us informed of changes to your business, plus other information including authorisation telephone numbers and what to do if your business experiences financial difficulties.

Notifying us of changes to your business

When writing to notify us of any changes, please send updated details on company headed paper.

Change of bank and/or branch

You must contact the Cardnet Helpline immediately on **01268 567 100** if your bank account details have changed. If you do not tell us there will be a delay in funds reaching your account. Changes to bank account details must be confirmed in writing. In certain situations we will also need a new Direct Debit mandate.

Change of address

You must notify Cardnet immediately and confirm in writing if you change your business or registered office address (or any other contact address you have asked us to use).

Closure or change of ownership

Your Cardnet facility is not transferable to anybody under any circumstances without Cardnet's written agreement. If you are selling or closing your business you must let us know in writing.

If the purchaser of your business wishes to use Cardnet, a new account will have to be opened that reflects the new ownership and we will make our usual pre-contract enquiries. If you fail to tell us that you no longer own the business you will continue to be liable for any liabilities that the subsequent owner(s) generate.

Change of legal entity

If you are changing the legal entity of your business, for example, from sole trader to limited company status, adding a partner to your business or if a partner leaves, you must let Cardnet know in writing immediately.

In most cases we will (subject to the usual risk checks) ask you to sign a new retailer agreement and Direct Debit mandate (in the name of the new entity) and depending on what other changes may have occurred, we may ask you for further information in order that we may conduct a further risk assessment.

Change of products or services sold or other details

When you join Cardnet you give us various product details that your business sells and we categorise your account accordingly. These details, including your card turnover and average sale value, are important in terms of the ongoing risk assessments that Cardnet regularly undertake.

Therefore, it is important that you let us know, in writing, if the nature of your business changes, for example, a change of product or service or if you expand into an additional line of business, different from your existing business. You must also tell us in writing if any of the other details that you have provided to us, whether in your application or otherwise, change.

If you do not tell us about any change, we may withhold our services or settlement payments pending our investigations and reassessment of risk.

Changing your trading terms

You must let us know immediately if you make any changes to your trading terms, for example, any changes to your Refund policy, or to the terms and conditions issued to your customers, or to the delivery time frames you have previously notified us of.

Write to us at:

Cardnet Merchant Services
Janus House
Endeavour Drive
Basildon
Essex SS14 3WF

Other changes affecting your business

You must tell us immediately if any of the following events occur:

- Any insolvency event affecting your business.
- You make any arrangement with creditors.
- You experience any financial difficulties.

Changing method of taking cards

If you would like to change your method of taking cards – either to Card Not Present or E-commerce transactions, you must have Cardnet's written agreement. For further details on changing your method of taking cards, contact the Cardnet Helpline on **01268 567 100** or write to us at the address above.

How to complain

Is there something you're not happy with?

Cardnet aims to give you the highest level of service. So if we make a mistake, or if there is something you feel we could do better, please tell us and we'll do our best to put it right.

This is to let you know what to do if you're not satisfied with the service we provide and the steps we ask you to take to help us deal with your complaint as quickly as possible.

Remember, most problems that arise can be resolved quickly if you talk to us as soon as possible.

When you call us you will need to have your merchant account number(s) to hand. Please remember, for security reasons, never to send this information to us by email.

Contact us

We need to know the nature of your complaint and how you think the problem should be resolved.

You can do this by:

Telephoning our Cardnet Helpline on **01268 567100.**

Emailing us at **cardnet_complaints@lloydsbanking.com**

Writing to us at the following address:

Lloyds Bank Cardnet
Phoenix House
Christopher Martin Road
Basildon
Essex SS14 3EZ

Our promise

We will always try to resolve your issue promptly. As soon as we have received your complaint we will respond to it as quickly as we can, usually by the end of the next working day. If we can't respond within this time (for example, we may need to refer your complaint to a specialist area), we will write to you within five working days to either:

- tell you what we have done to resolve the problem; or
- acknowledge your complaint and let you know how to contact the person or team dealing with your case.

- **We will also:**
- Provide you with regular updates.
- Let you know our final response within eight weeks from when you first contacted us about your complaint.

Contact the Financial Ombudsman Service

If you remain dissatisfied:

You may be able to refer your case to the Financial Ombudsman Service for an independent review. This is a free, independent dispute resolution service for customers of most UK banks, building societies, insurance companies and other financial institutions.

Their details are as follows:

Financial Ombudsman Service
South Quay Plaza
183 Marsh Wall
London E14 9SR
Telephone **0800 0234567** (from a landline) or **0300 1239123** (from a mobile).

You will find more information on the Financial Ombudsman Service website, including details about eligibility at **www.financial-ombudsman.org.uk**

We value your custom and want to resolve your complaint for you. The Financial Ombudsman Service will only consider your complaint once you've tried to resolve it with us or no final response has been provided after eight weeks from the complaint being made.

What to do if you experience financial difficulties

You will usually spot financial problems before us and you should let us know of your difficulties as soon as possible.

If we become aware of problems we will let you know in writing.

Chargebacks will usually be the main reason for financial problems connected with your card acquiring facility, which is why it is important that you follow the procedures outlined in the manual carefully. The most common type of chargeback is in respect of CNP transactions where you need to be particularly vigilant to avoid being targeted by fraudsters. See Section 7, 'How to guard against fraud' (p75). Most other chargebacks arise when transactions have not been read through the terminal, imprinted or authorised correctly.

This list gives a few examples of problems that can concern us, particularly if you do not explain what is happening:

- There is a large increase in your card turnover.
- The value of a transaction is significantly larger than you told us you would process or usually process.
- There are unusual numbers of 'key entered' transactions.
- We start to see chargebacks from issuers on your account particularly if cardholders are not receiving goods that they have ordered.
- Transactions are not being correctly authorised.
- Direct Debits are returned unpaid by your bank branch.

We can offer guidance to help protect you from financial loss. If you are concerned about fraud, we can send you training information and materials. If you are concerned about suffering a chargeback, or experience financial difficulties as a result of a chargeback, we will do all we can to help you. We will also try to reach agreement with you on how and when debts will be repaid and tell you where you can get advice – see page p109 for details. We will be happy to work with your advisers in order to reach a satisfactory conclusion to your difficulties.

Financial implications of Cardnet

If you are a sole trader you are liable for any debts that may arise under the retailer agreement that you signed when joining Cardnet.

If you are a partner in a business, or a trustee or committee member of a charity or club/society, you are jointly and severally liable for any debts or other liabilities that may arise under the retailer agreement from using our services. Each of the partners, trustees or committee members is separately responsible for keeping to its terms and repaying any debts or other liabilities and not just a share of it, even though they may not be a signatory to the retailer agreement. If any of you fails to comply with them, we can take action against one or more or all of you either individually or together. For example, we can take action to recover the whole of any debt from any one or more or all of you. If we are owed money when a partner, trustee or committee member dies, the deceased's estate remains responsible for paying the debt and we may require payment from it.

If we are owed money when a partner, trustee or committee member leaves the business, trust fund, charity or club/society, the outgoing partner, trustee or committee member remains separately responsible to repay the existing debt.

If you are a director of a limited company or a member of a limited partnership, your personal liability to Cardnet under the retailer agreement is limited to the capital you have invested in the company or partnership. Under the terms of the retailer agreement, the company or limited liability partnership will be fully liable for any debts arising under the agreement.

Agencies offering financial assistance

You may find the following phone numbers and websites useful.

Business Debtline
0121 250 3000 (www.birminghamsettlement.org.uk)

Gov.UK
0845 600 9006 (www.gov.uk)

Citizens' Advice Bureaux
(www.citizensadvice.org.uk)

Citizens' Advice Scotland
0808 800 9060 (www.cas.org.uk)

Federation of Small Businesses
0808 202 0888 (www.fsb.org.uk)

Financial Conduct Authority (FCA)
0845 606 9966 (www.fca.org.uk)

Prudential Regulation Authority
020 3461 7000 (www.bankofengland.co.uk)

National Federation of Enterprise Agencies
01234 831 623 (www.nfea.com)

Northern Ireland Association of Citizens' Advice Bureaux
028 9023 1120 (www.citizensadvice.co.uk)

The British Chambers of Commerce
0207 654 5800 (www.britishchambers.org.uk)

The Insolvency Service
0845 602 9848 (www.insolvency.gov.uk)

The Forum of Private Business
0845 130 1722 (www.fpb.org)

The Institute of Directors
0207 766 8866 (www.iod.com)

Authorisation telephone numbers

Over the counter (OTC) sales

01268 822 822

Card Not Present (CNP) transactions

01268 278 278

Lines are open 24 hours, Monday to Sunday.

Merchant services

Cardnet Helpline – For any queries with your Cardnet account, please telephone

01268 567 100

Lines are open 8am to 9pm, Monday to Saturday.

Alternatively, you can write to Cardnet at the following address:

Cardnet Merchant Services
Janus House
Endeavour Drive
Basildon
Essex SS14 3WF

Please ensure that all Cardnet related enquiries are referred to Cardnet. You should not seek advice or guidance in respect of Cardnet issues from your local branch or manager.

Cardnet stationery

Stocks of stationery, i.e. Sales, Refund and Summary Vouchers, and deposit envelopes, are available by completing the re-order form which you'll find in each box of vouchers. Simply place the completed re-order form behind the Sales Vouchers when sending into Cardnet.

Please be aware that we can only accept paper transactions made on official Cardnet stationery.

In an emergency, vouchers can also be ordered by telephoning **01268 296 601** (24-hour answerphone service). You will be required to give your Cardnet merchant number.

Point of sale and display material

A varied selection of point of sale material such as tent cards, window and till stickers are available by telephoning the Cardnet Helpline on **01268 567 100**.

Recommended tally roll supplier

Primatel

For further supplies of tally rolls, call Primatel direct on:

Tel: **0845 430 1379** or **020 8679 4428**

Lines are open 9am to 5pm, Monday to Friday.

Fax: **020 8679 4420**
E-mail: **enquiries@primatel.co.uk**
Website: **www.primatel.co.uk**

Cards left on your premises

Any cards left at your premises must be kept safely until the end of business on the day when the card was found. If the cardholder returns to claim the card, you must obtain the claimant's signature and compare this signature with that on the card. If you are suspicious that the claimant is not the cardholder, you must telephone the Authorisation Centre and state "This is a Code 10 call". Only release the card if you are satisfied that the claimant is the cardholder. Unclaimed cards should be cut across the bottom left-hand corner of the front of the card and both parts attached to a Cardnet Card Recovery Advice Form. Please complete the form and send it to:

Cardnet Rewards Department
Merchant Operations
Janus House
Endeavour Drive
Basildon
Essex SS14 3WF

A financial reward is not given in these circumstances.

Emergencies and disruptions

In case of any disruptions to the postal or telephone services, you should hold a supply of Sales Vouchers and banking stationery.

If a disruption does occur, the following procedure will apply:

- Your Cardnet statement will be sent to you as soon as possible.
- As your account is settled by Direct Debit to your bank, this will continue to be done and we will notify you as soon as possible.
- You will be able to continue monitoring credits received by Cardnet by checking your bank statement.
- Chargebacks will be processed in the normal way but you will not be able to receive details until the emergency or disruption is over.

Our service promise. If you experience a problem, we will always try to resolve it as quickly as possible. Please bring it to the attention of any member of staff. Our complaints procedures are published at lloydsbankcardnet.com/contactus

Important information

Calls may be monitored or recorded in case we need to check we have carried out your instructions correctly and to help improve our quality of service.

Please remember we cannot guarantee the security of messages sent by email.

Cardnet® is a registered trademark of Lloyds Bank plc. MasterCard® and the MasterCard Brand Mark are a registered trademark of MasterCard International Incorporated, Maestro® is a registered trademark of MasterCard International Incorporated.

Lloyds Bank plc. Registered Office: 25 Gresham Street, London EC2V 7HN. Registered in England and Wales No. 2065. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.

Lloyds Bank plc is covered by the Financial Ombudsman Service. (Please note that due to the eligibility criteria of this scheme not all Lloyds Bank customers will be covered.)

This information is correct as of September 2013.

Get in touch

Go to lloydsbankcardnet.com

Call us on 01268 567100

Lines open 8am–9pm Monday to Saturday

Please contact us if you'd like this information in an alternative format such as Braille, large print or audio.

LLOYDS BANK

CARDNET

CMS200 (09/13)